優先権主張
国名 アメリカ合衆国
出願 1974年6月25日
出願番号 オ 483084 号

特許願(4)

昭和50年6月4日

特許庁長官 斎藤英雄 殿

1.発明の名称 トリヒキジッコウ
取引実行システム

2.発明者
住所 アメリカ合衆国カリフォルニア州ロス・アルトス
ハイエラ・コート851番地
氏名 トーマス・ジー・アンダーソン (他2名)

3.特許出願人
住所 アメリカ合衆国10504、ニューヨーク州
アーモンク(番地なし)
名称 インターナショナル・ビジネス・マシーンズ・コーポレーション
(709)
代表者 ジェイ・エイチ・グレイデイー
国籍 アメリカ合衆国

4.代理人
郵便番号 106
住所 東京都港区六本木三丁目2番12号
日本アイ・ビー・エム株式会社
Tel (代表) 586-1111 (内線2265)
氏名 弁理士 小野 廣司
(6454)

5.添付書類の目録
(1) 明細書 1通
(2) 図面 1通
(3) 委任状及訳文 各1通
(4) 優先権証明書及訳文 各1通
(5) 出願審査請求書 1通

特許庁 50.6.4 出願第二課

⑲ 日本国特許庁

公開特許公報

⑪特開昭 51-6632
⑬公開日 昭51.(1976)1.20
㉑特願昭 50-66660
㉒出願日 昭50.(1975)6.4
審査請求 有 (全33頁)

庁内整理番号
6372 56
6127 56

㊷日本分類	㊶Int.Cl²
97(7)J1 97(7)D3	G06F 15/30 G06F 3/00

明細書

1.発明の名称 取引実行システム

2.特許請求の範囲

第1の情報ブロック及び予め決められたエンコード方式に従つて第3の情報ブロックを暗号化することによつて得られる第2の情報ブロックを夫々含む複数の取引勘定情報を保持しており、要求された取引に関連する取引勘定情報に対する上記第1及び第2の情報ブロックが受信された取引要求メッセージの一部に含まれているときにのみ上記要求された取引を承認し且つこれに関連する取引勘定情報を上記要求された取引の内容に応じて変えるように動作しうる主データ処理システムと、

顧客から取引要求情報と共に取引勘定情報に対する上記第1及び第3の情報ブロックを受取るように動作し、上記第2の情報ブロックを発生するように上記予め決められたエンコード方式に従つて上記受取られた第3の情報ブロックを暗号化する手段、並びに上記取引要求情報、第1及び第2の情報ブロックを取引要求メッセージとして上記主データ処理システムへ伝送する手段を含む少なくとも1つの取引用端末装置とよりなる取引実行システム。

3.発明の詳細な説明

本発明は取引実行システムに係り、更に具体的に言えば中央処理システムにデータ・ベースを有し、取引例えば現金の支払又は資金を1つの勘定から他の勘定へ移すことを実行したい遠隔端末装置と上記中央処理システムとの間で通信する取引実行システムを保護することに係る。

公衆の便宜及び経済性に関する理由から、顧客が要求した取引を実行する種々のシステムが開発されている。その1つの例は小切手現金化装置である。このような装置はその中へ差込まれた小切手からのデータを読取つて、もしその小切手に対して現金を支払つてもよいということが見出されたならばその小切手相当額の現金を支払う。又、クレジット・カードに関連して使用するための他のシステムが開発されている。

1つのクレジット・カード・システムは中央処理システムのデータ・ベースにクレジット・カード勘定情報を貯えている。遠隔端末装置からクレジット・カード・システムへ勘定番号が送られて来ると、該システムはその勘定番号に関係する情報を送出する。例えば、クレジット・カード・システムはそのカードが効力を失くしている若しくは盗難に会つているということを示してもよいし、又はそのクレジット・カードで利用しうる金額を示してもよい。取引が完了した後、クレジット・カード・システムは取引高の勘定を付けるように貯えられている情報を適正に書き直す。

多忙な営業時間中や営業停止時間中までも銀行業務のサービスを提供するのに銀行によつてしばしば使用される他のクレジット・カード・システムは現金を支払つたり、端末装置を介して預金を受付けたりする。このような端末装置は代表的には、クレジット・カードへ情報を与えたり該カードから情報を読取つたりする機構、キーボード、データ表示装置並びに文書挿入兼排出口を含む。この端末装置はデータ・ベースに関連して又は単独のユニットとして動作してもよい。人手にたよることなしに現金支払の安全性（機密性）は各々のクレジット・カードに個人何定番号（以下、個人ＩＤ番号若しくはＩＤ情報（ＩＤ番号）とも呼ぶ。）を付することによつて高められる。クレジット・カードから読取られた勘定番号に対応するＩＤ番号がキーボードから打込まれたときにのみクレジット・カードによる取引が行われうる。この必要とする対応付けがクレジット・カードの盗人又は単なる発見者には端末装置から現金を受領させない。端末装置がデータ・ベースに関連して動作するならば、勘定番号とＩＤ番号との間の対応は無差別に選ばれるが、ＩＤ番号が予め決められたコードに従つて勘定番号から得られる方が多い。この予め決められた関係はＩＤ番号をアルゴリズムで勘定番号に関係付けることによつて単独の端末装置においてＩＤ番号を検査させる。

このクレジット・カードからの勘定番号とＩＤ番号の2つによる同定技法は現金支払端末装置の安全性（機密性）を高めるが、端末装置に貯えられている高額の現金をアクセスしうるような装置を開発したい場合に依然として弱点を有する。例えば、データ・ベースを有する中央処理システムにおいては相当数のコンピュータ・オペレータ、プログラマ、分析者及び他の人々（中央処理システムのデータ・ベースに貯えられた情報に対し少なくとも限られたアクセスをしうるだけである。）を雇う必要がある。これらの要員のいずれかの人が偽造の若しくは盗難に会つたクレジット・カードに関連する勘定番号及び対応するＩＤ番号をコンパイルし使用して現金を得ることは可能である。

同等に重大な問題は単独に動作しうる端末装置のための暗号化アルゴリズム（encryption algorithm）の安全性（機密性）に関係している問題である。多数のオペレータ若しくは保守要員が現金支払端末装置を毎日保守するのに必要である。例えば、銀行の各支店で1人若しくは2人が現金支払装置の、通常ではアクセスしない部分へアクセスすることがある。しばしば、これらの人は通常の保守のため上記アルゴリズムの暗号キー部分へアクセスすることがある。又、僅かに訓練を受けた状態の下でも、これらの人々は装置の内部回路の種々の電気信号を測定することによつて上記の暗号キー部分へアクセスしうることができる。一旦この暗号キー部分がアクセスされると、多数の勘定番号と多数のＩＤ番号との対応が見出されるようになる。

他の起りうる安全性（機密性）の問題は端末装置とデータ・ベースを有する中央処理装置との間で勘定情報及びＩＤ情報を伝送する際に生ずる問題である。この伝送はしばしば公共の伝送線を介して行われ、そのため多数の人によつて傍受され易い。暗号化手段は伝送の安全性（機密性）を高めるのにしばしば用いられるが、暗号化コードを知り得る若しくは該コードをアクセスしうる何人も上記伝送線を介しての伝送を傍受すればクレジット・カードの勘定情報及びＩＤ番号を抽出してこれらの間の対応リストをコンパイルしうる。これに加えて、端末装置からにせの通信トラヒック

を生じさせた場合に、人が中央処理システムのデータ・ベースへアクセスしうることがあり、データ・ベースの勘定内で資金をごまかしてやりとりしうることがある。従つて、これらの２つの情報を用いる同定技法を用いる通常のシステムは通常の盗人に対しては保護されうるが、現代のデータ処理装置に関する知識を有する知能犯に対しては、この通常のシステムは適切に保護されなくなる。

本発明になる取引実行システムは多くの勘定番号に対する情報を貯えているデータ・ベースを有する主データ処理システム並び複数の取引用端末装置を含む。主データ処理システムは提示されている取引を容認若しくは否認し、実行された取引を適正に記録するように貯えられた勘定情報を更新し、端末装置のための支援情報を発生する。取引用端末装置は動作上、分散した位置から主データ処理システムとデータの受授を行うように接続されている単独のユニットである。各々の端末装置は現金支払取引書若しくは取引伝票のための取引書取扱いサブシステム、クレジット・カード読取サブシステム、主データ処理システム－端末装置間通信サブシステム、顧客－端末装置間通信サブシステム、並びにプログラム可能なマイクロプロセッサを含む動作制御サブシステムを含む。

取引書取扱いサブシステムは現金貯蔵機構、マイクロプロセッサの管理及び制御の下に現金を顧客に支払うための現金輸送機構、並びにマイクロプロセッサの制御の下に印刷された取引書を発行する取引書発行装置を含む。クレジット・カード読取サブシステムは取引の要求を処理した後返却しても又は保持してもよい顧客のクレジット・カードを受取り読取るようにマイクロプロセッサの制御の下に動作する。主データ処理システム－端末装置間通信サブシステムは予め決められた通信フォーマットに従つて端末装置と主データ処理システムとの間で情報を適正に送受するためのインターフエイスとなる。顧客－端末装置間通信サブシステムはマイクロプロセッサの制御の下に端末装置への顧客によるアクセスを制御するように動作し、顧客の要求事項を打込むためのキーボード及び相互作用の下に顧客に必要な事項を与えるための表示装置を含む。

取引を実行したい顧客は端末装置のクレジット・カード読取サブシステムの中へクレジット・カードを挿入し、然る後に当該顧客ＩＤ情報及び取引要求情報をキーボードを介して打込まなければならない。然る後に、端末装置はキーボードから打込まれたＩＤ情報の選ばれた部分との対応につきテストされるところの暗号化されたＩＤ情報を得るように第１の暗号化用キーを使つてクレジット・カード情報の選ばれた部分を随意にエンコードする。予め決められた対応が両者の間になければ、取引は停止され、主データ処理システムはメッセージを介して知らされ、主データ処理システムからの返答によつてそのカードに対する処置が取られ、そのカードは返却されるか、保持される。上記の対応が見出されるならば、第１の暗号化用キーと同じであつてもよい第２の暗号化用キーを使つてキーボードから打込まれたＩＤ情報はエンコードされる。暗号化されたＩＤ情報は同一の号化されたフイールドを繰返して転送させないためにシーケンシヤルな取引番号若しくは現金カウントのような可変の情報と結合され、然る後に転送のための第３の暗号化用キーを使つて再びエンコードされる。この暗号化プロセスは主データ処理装置のデータ・ベースをしてＩＤ番号を貯えさせるのではなく、暗号化されたＩＤ番号だけを貯えさせる。かくして、このデータ・ベースはにせのカードから作られる勘定番号とＩＤ番号との対応リストの不正な抽出に対して保護される。暗号化されたＩＤ情報はクリア・テキスト要求情報及びクレジット・カードから読取られた情報と結合され、そして主データ処理システムへ送られる。３つの部分から成る取引実行シーケンスは、可変データと結合されそして再度暗号化されるところの暗号化されたＩＤ番号、クレジット・カードから読取られた情報並びにキーボードから打込まれた取引要求情報を主データ処理システムへ与える取引要求メッセージで始まる。例えば、顧客が自分のクレジット・カードの勘定から＄１００の支

払いを要求するものとする。要求が主データ処理システムで受取られると、主データ処理システムはエンコードされ伝送されて来たＩＤ番号と主データ処理システムのデータ・ベースに貯えられているところのエンコードされたＩＤ番号との対応を調べ、勘定制限事項例えばクレジット・カードに対し支払われる最高現金高を調べ、そしてこれらのことがすべて整うならば取引を認める取引返答メッセージを端末装置へ送り、逆に整わないならば主データ処理システムは要求された取引を認めない。

取引要求メッセージと同様、主データ処理システムから上記取引要求メッセージに対する取引返答メッセージはアクション・コマンド（行動指令）及び可変データ例えば現金カウント数若しくは取引番号を含む暗号化された部分を含む。このエンコードされた情報はクリア・テキスト情報例えば取引書情報及び表示情報と結合された後、返答メッセージは要求を出している端末装置へ送られる。

取引返答メッセージが要求を出している取引用端末装置によつて受取られると、該端末装置は上記取引返答メッセージを暗号解読し、エラーがあるか否かについて可変データの正しさをチエックし、然る後に指令された行動を実行する。然る後に、端末装置は取引の実行若しくは取消し並びに端末装置での何らかのエラー状態を主データ処理システムへ知らせるようにステータス・メッセージを発生する。このステータス・メッセージの暗号化された部分には取引番号、該メッセージ内のステータス・バイト数、及び現金カウンタ・ステータスを含む。主データ処理システムは取引の内容を記録し又はデータ・ベースを更新することによつて提示された取引の勘定を適正に記録するように動作する。エラー状態が見出されるならば、主データ処理システムはコマンド・メッセージを送り出し、そのエラーを正すように試みるか、又はそのエラーが正され得ない場合にはその端末装置の機能を停止する。このデータ・メッセージ技法を用いれば、暗号化用キーは非常に見出し難くなり、又主データ処理システム及び端末装置が正しいメッセージに応答することを保証するように冗長性をもつて通信（データの送受）が行える。これに加えて、顧客ＩＤ番号と勘定番号との間の対応がこれらの番号を主データ処理システムのデータ・ベースに貯える必要性を除く暗号化技法によつて保護される。

本発明になる取引実行システム１０は主データ処理システム１２並びに該システムとの間で通信する複数の顧客取引用端末装置１４を含む。主データ処理システム１２は主中央処理ユニット（ＣＰＵ）１６例えばＩＢＭシステム３７０、通信制御装置１８例えばＩＢＭ３７０５並びに電気的に更新可能なランダム・アクセス・メモリ、磁気テープ記録装置、及び磁気ディスク装置から成つてもよいデータ・ベース２０を含む。主ＣＰＵは主データ処理システム１２の動作を制御し、通信制御装置１８を経て受取られ又はデータ・ベース２０に貯えられている情報を処理するのに必要な算術演算及び論理演算を実行する。データ・ベース２０は主データ処理システム１２の各々の顧客に関連付けられる情報を貯える。例えば、銀行の顧客に対しては、上記のデータ・ベースはクレジット・カードのための勘定情報、貯金、小切手、又は銀行の他の勘定事項、そして給料支払情報及び銀行の営業に関する金融上の状態に関係する情報を貯えてもよい。各々の勘定項目は代表的には勘定番号によつてアドレス可能であるのがよく、勘定番号に従つて現時点での勘定情報例えば現時点での残高、予め決められた時間期間に亘る取引勘定の経過、銀行の勘定項目を使用してもよい顧客のための符号化された顧客用ＩＤ番号、クレジット・カードの最高支払高、銀行が勘定項目の一部として貯えたいその他の任意の情報を貯えている。通信制御装置１８はＣＰＵ１６と複数の通信チャネル２０との間のインターフエイスとして働く。制御装置１８は自身を経由する情報を通信方式に合うように再組立し、そして通信の同期を維持する。

取引用端末装置１４は種々の方式で第１図の例示としてのみ示されている殆んど制限されない数の経路を経て主データ処理システム１２と通信を

行いうる。例えば、端末装置は近隔の顧客取引用端末装置２６に対しては近隔通信リンク例えばケーブル２４又は遠隔の顧客取引用端末装置３０に対しては公共施設リンク若しくは無線リンク２８を経て通信制御装置１８へ直接に接続されうる。又は、端末装置３６に対してケーブル３４を経て接続されるように制御装置３２へ直接に接続すること又は通信ループ３８内に接続することによつて端末装置は制御装置３２例えばＩＢＭ ３６０１を経て主データ処理システム１２へ接続されてもよい。他のデバイスが含まれてもよいが、通信ループ３８は第１の話者作業ステーション４０、第２の話者作業ステーション、第１の顧客取引用端末装置４４及び第２の顧客取引用端末装置４６を含むものとして例示されている。通信ループ３８はバンキング・システムに対しては遠隔通信リンク例えば無線による通信、又公共施設の伝送線を経ての通信を含みうるが、銀行の支店に設置されたすべてのデータ処理端末装置を通信ループ１８に接続するように上記支店毎に制御装置３２が代表的に設置される状態で制御装置３２が上記支店に設置されるのがよい。制御装置３２自身は通信リンク４８例えば第１図に示される公共施設の通信線を経て通信制御装置１８の通信チャネル２２へ直接に接続されるか、又は通信ループ例えば通信制御装置１８のデータ送受チャネル２２へ通じているループ３８へ接続されるのがよい。

一般的には、制御装置３２は単に、ループ３８を通る情報のための中継デバイスとして働くが、主データ処理システム１２との直接的で実時間の通信が維持されない場合には主データ処理システムとして動作してもよい。主データ処理システムとして動作する場合には、制御装置３２は主データ処理システム１２による後刻における処理のための取引実行情報を貯えていなければならず、又端末装置１４の動作に必要な主データ処理システムに対する支援機能をも備えていなければならない。

取引実行端末装置

取引用端末装置１４が施行される特定の様式は本発明を実施する上では重要ではないが、端末装置１４の良好な実施例が第２図に示されている。端末装置１４は全体をモジュールで構成されており、情報バス６２を経て複数の端末装置サブシステムへ接続されたプログラム可能なマイクロプロセッサ６０を含む。マイクロプロセッサ６０はクロック信号発生器６４からのクロック信号によつて駆動され、又動作に従つて、電気的に更新可能なランダム・アクセス・メモリ（ＲＡＭ）及び読出専用メモリ（ＲＯＭ）を備えているデータ貯蔵モジュール６６のどちらかのメモリへ接続される。データ貯蔵モジュール６６の読出専用部分はマイクロプロセッサ６０のための種々のオペレーティング・プログラムを貯えている。データ貯蔵モジュール６６のランダム・アクセス・メモリ部分はプログラム実行のためのスクラッチパッド・メモリである。ＲＡＭが代表的なＩＣメモリの場合には、ＲＡＭの内容は電源がなくなれば失われる。

端末装置内情報バス

マイクロプロセッサ６０は端末装置内情報バス６２を経てのみモジュール化されたサブシステムと通信する。モジュール化されたサブシステムの各々をバス６２を経てマイクロプロセッサ６０に相互接続するこの技法は、マイクロプロセッサ６０に端末装置ステータスに関する詳細な情報を受取らせ、多数の入出力接続なしに端末装置内のハードウエアの諸動作を詳部に亘つて指揮させる。端末装置のステータス情報を感知するタスク（仕事）は端末装置内の個々のサブシステムによつて遂行される。この感知されたステータス情報はマイクロプロセッサ６０からの指令（コマンド）に従つてマイクロプロセッサ６０へ転送される。同様に、マイクロプロセッサのコマンドを実行するための駆動回路及びハードウエアはサブシステムを構成するモジュール内に含まれている。マイクロプロセッサのコマンドはその性質上極めて基本的で動

作の詳細を規制するものである。各々のコマンドはサブシステムの基本的な動作例えばモータの附勢又は消勢、文字の表示若しくは印字、勘定書の給送、又は送信する文字の読取を遂行させる。情報バス６２はシステム・リセット信号、マイクロプロセッサ６０へ情報を転送するための９つのデータ入力信号（８つのデータ・ビット及び１つのパリテイ・ビット）、マイクロプロセッサ６０からの情報を動作に従つて接続されるサブシステムへ転送するための９つのデータ出力信号（８つのデータ・ビット及び１つのパリテイ・ビット）、並びに情報をバス６２へ転送し、又は情報をバス６２から転送するのを制御するバス制御信号を運ぶ。

マイクロプロセッサ支援サブシステム

バス６２を経てマイクロプロセッサ６０へ接続される各々異なる機能を果たす諸サブシステムの内の１つはマイクロプロセッサ支援サブシステム６８である。端末装置１４の諸動作の内の特定の動作に関係する機能を夫々果たすところの端末装置内の他のサブシステムに対して、マイクロプロセッサ支援サブシステム６８はマイクロプロセッサ６０に対しハードウエア上の補佐機能を有する。

マイクロプロセッサ支援サブシステム６８はクロック信号発生器６４からの１ MH_z のクロック信号を受信し、該クロック信号を分周して他の夫々のサブシステムで用いられる上記クロック信号より低い周波数のクロック信号を発生する。より低周波の１つのクロック信号は１０msecの間隔で周期的割込コマンドを発生するのに用いられる。これらの割込コマンドはマイクロプロセッサ支援サブシステム６８内の割込論理部をして１０msec毎にマイクロプロセッサの割込を発生させる。マイクロプロセッサ６０はこれらのクロック信号による周期的な割込を利用して端末装置１４の種々の動作のための事象制御時間基準を維持する。サブシステム６８内のリセット論理部は情報バス６２のリセット線を制御する。このリセット線が附勢されると、マイクロプロセッサ６０並びにバス６２へ接続されているすべてのモジュールの初期状態を生じさせ、どのような進行中の、顧客による取引も取消される。マイクロプロセッサ６０はプログラム内の予め決められた命令へ戻り、上記のリセットに続いて上記命令からプログラムの実行が再開される。リセット信号は交流電源から供電、リセット・スイッチ、又はサブシステム６８内の休止検出器からの休止信号に応答して発生される。休止検出器はバス６０内の制御信号をモニタし、マイクロプロセッサ６０が適正に動作していないということを示すのに十分な時間の間バスの活動が止むときに休止信号を発生する。動作継続検出器はタイマ割込要求信号に応答してマイクロプロセッサが規定通りに諸要求に応答している限り、活動状態に維持される動作継続信号を発生する。タイマ割込要求の処理なしに予め決められた時間期間が経過したならば、動作継続検出器は動作継続信号を発生しなくなる。サブシステム６８は、また、顧客のクレジット・カードから読み取られる一連の直列情報を受け取り、データをクロック情報から分離し、直列の２進ビットを並列化し、マイクロプロセッサ６０による処理のため並列化された情報をバス６２を経て送り出す。

機構制御サブシステム

機構制御サブシステム７０は端末装置１４の種々の機構の機械的制御を行う。他のサブシステムのような分岐機能、若しくは判断機能を持たないサブシステム７０はマイクロプロセッサ６０から基本的で初歩的なコマンドを実行し、マイクロプロセッサ６０へ送るための種々の機構の物理的なステータスに関する情報を収集する。機構制御システム７０によつて実行される個別の機械的な性質の諸機能の例としては、クレジット・カード操作機構はクレジット・カードの動きに応答してコマンドを発生して読取ヘッドの下にクレジット・カードを移送して来るようにカード移送機構を駆動するモータを附勢する。複数の感知器（スイッチ若しくはホトセル）が(1)挿入位置、(2)排出ジャム感知位置、及び(3)カード保管位置にクレジット・

カードがあるか否かを感知するように夫々設けられる。感知器が働くと、それを示す情報ビットがステータス・ワードの中に設定される。マイクロプロセッサ６０が既取動作中に周期的に種々のステータス・ワードを調べ、クレジット・カードがそれを置く保管部に到達しているかどうかを決定する。然る後に、マイクロプロセッサ６０はクレジット・カード移送モータに制動をかけられるように短い時間の間該モータを逆転させる制御信号を出し、然る後にモータの附勢を停止する制御信号を出す。類似の初歩的な方式で、サブシステム７０はクレジット・カードの操作段階を終了させる操作例えばクレジット・カードの保管又は顧客への返却を制御する。その他の機能は顧客が決してアクセスし得ない保管部へ顧客が取引書を預けたい場合にその保管を制御することを含む。同様に、サブシステム７０は顧客がアクセスしうるドアの開閉、印刷された取引書を現金と共に置く場所への予め決められた額の現金の送出、上記場所へ置かれる取引書の発行若しくは保管を制御する。

サブシステム７０によつて制御される機構のステータスを感知することに加えて、該サブシステムは現金支払機 に貯えられている現金の存在を感知し、取引のため支払われる現金の最高額を支払い得ないとき表示信号を発生する。サブシステム７０は又遠隔の制御パネル及びマイクロプロセッサとの間の通信のための諸状態を感知する。遠隔からのこれらの信号はサービス・ドアが開かれているか否かの表示信号、侵入感知格子が防害されていないか否かの表示信号、介入を必要とする状態が存在するか否かの表示信号を含む。遠隔のパネルへ送られる他の信号は取引書フォーム若しくは現金量減少に関する信号、サービス・ドアが開かれオペレータがアクセスしていることを示す信号、端末装置と応答しうる状態にある主データ処理システムとの間の通信に関する信号を含む。遠隔のパネルに設けられているコマンド・スイッチには、端末装置リセット・スイッチ、及び通信リンクのテストを指揮するラップ・スイッチ（wrap switch）を含んでもよい。

顧客－端末装置間通信サブシステム

顧客－端末装置間通信サブシステム７２は端末装置１４と顧客との間の２方向の通信を制御する。通信サブシステム７２は顧客が発生したいコマンドを打込むためのキーボード、２２２の水平方向ドット×７ドットを表示しうる表示装置を含み、そして表示装置制御論理回路及びリフレシュ・バッファを含む。表示装置制御論理回路は特定の表示したいドット像を受取り、表示停止コマンドが受信されるまでその表示を続ける。

キーボードは複数のフィールドに分けられており各フィールドには複数のキーがある。例えば、取引選択フィールドは顧客が実行したい取引の型式を示す。他の諸フィールドの夫々は例えば、預金から現金を引出したいことを示す引出選択フィールド、現金を預金したいことを示す預金選択フィールド、並びに１０進数例えば、顧客ＩＤ番号、若しくは現金高を打込むための数字キーボード・フィールドである。取引選択キー、預金選択キー、引出選択キーにはバック・ライトが設けられており、これらのキーは、既に使用されたフィールドのどのキーが選ばれたかという確認表示を顧客に知らせるためのものである。次にキーが作動されるフィールドの中のすべてのバック・ライトが点灯される。例えば、顧客が自分のクレジット・カードを端末装置へ入れてから、自分のＩＤ番号をキーから打込む。ＩＤ番号が適正に受取られた後、取引選択フィールドのすべてのキーが点灯されるようになる。顧客が特定のキー例えば'funds transfer'キーを作動させると、該キーのバック・ライトのみが点灯されたままになつており、その他のすべてのバック・ライトは消灯される。次のフィールド例えば引出フィールドのすべてのキーのバック・ライトが取引要求に関する次のステップの準備のため点灯される。この方式において、先行する夫々のフィールドのキーが作動された確認表示が与えられ、次に選択すべきフィールドが指示される。顧客に適当な順序を与えるために表示メッセージ及びカラー・コーディングが

用いられてもよい。顧客－端末装置間通信サブシステム７２のキーボード制御論理回路はマイクロプロセッサ６０によつて制御される特定のキーのバック・ライトを点灯し、又どのキーが顧客によつて作動されたかということをマイクロプロセッサ６０へ知らせるのに必要な回路を含む。

取引書発行サブシステム

取引書発行サブシステム７４は取引書を移送するための取引書操作機構、プリンタ、プリンタ制御論理回路、並びにサブシステム７４とバス６２とのインターフエイスとなる論理回路を含む。サブシステム７４は特殊で基本的なコマンド例えば移動の開始若しくは特定の文字の印字に関するコマンドに応答する。サブシステム７４はバス６２を経てマイクロプロセッサ６０と通信するため該サブシステムの機構の物理的なステータスに関する情報を収集する。この情報は特定の個々の機能の首尾よい完了を検出するようにプログラム制御の下に動作し、又次の機能の開始を指揮するマイクロプロセッサ６０によつて使用される。

オペレータ用機能サブシステム

オペレータ用機能サブシステム７６はオペレータによる保守のためのインターフエイスを与え、そして、複数の入力スイッチ、４デイジット１６進表示装置、電源感知回路、並びに複数のシステム・パラメータを貯え且つ例外情報を記録するのに用いられる停電時に確保される１２８バイト容量の補助メモリを含む。貯えられるパラメータは現金カウンタ数、複数の暗号化用キー及び取引番号を含む。オペレータ用パネルへのアクセスは端末装置１４の背後に設けられ顧客に対しては閉鎖されている二重閉鎖ドアを開くことによつてなされる。上記二重閉鎖ドアを開いて保守作業を試みようとする場合には、上記補助メモリに通常貯えられている暗号化用キーは破壊される。このような暗号化用キーの破壊によつて、電気的測定器具を使つて不揮発性メモリ（補助メモリ）内の暗号化用キーを探して読出そうとするオペレータから暗号化用キーは保護される。端末装置が応答され得るようになる前にこのような暗号化用キーは信用度の高い人によつてキーボードから送り込まれる。８バイトのキーの各々一時に２デイジットずつ１６の１６進デイジットとして送り込まれる。キーを見出そうとするもぐりの人に対して困難度を高めるためにこれらのキーが送り込まれるとき夫々の２デイジットずつだけが表示される。又は、勘定番号と顧客ＩＤ番号との対応を定めるキーＡは、該キーＡを作り出すためには、第４の暗号化用キーに従つて暗号化されるところの暗号解読化されたキー（キーＡ'）を送り込むことを必要とすることによつて更に一層保護されうる。この技法を使用すれば、実際のキーＡは端末装置１４が置かれている場所でのあらゆる人からその安全性を確保しうる。電源感知回路は公共施設からの交流電圧レベルと内部直流電圧レベルとをモニタしており、交流電源が停電となり直流電圧レベルが低いという事が感知される場合には、信号がマイクロプロセッサ６０へ送られ、動作上重要な情報を貯えさせ、然る後に補助メモリが補助電源でその機能を保つている間は、該メモリへのアクセスは制限される。論理回路のための直流電圧が適切な値にある限り、表示信号がオペレータ・パネルへ供給されている。

通信サブシステム

通信サブシステム７８は通信チヤネルと情報バス６２との間の通信のためのインターフエイスを与える。サブシステム７８は通常知られているものであり、一時に１バイト、情報バス６２から受取り又は該バスへ与える。

遠隔端末装置内信号コネクタ

遠隔端末装置内信号コネクタ８２は実際には端末装置１４の一部である遠隔制御パネルへ或る種のステータス信号及び或る種の制御信号入力を供給するように動作する。例えば、銀行の支店は５つの端末装置１４、並びに便宜上の主要な位置に設置された、５つの端末装置１４毎に光学的表示装置及び制御スイッチを有する単一の集中化され

た遠隔制御パネルを有するのがよい。遠隔制御パネルへのこれらの信号は主として端末装置の動作をモニタし、又は特別の状態を制御するための信号であり、顧客の通常の取引には用いられない。特定の遠隔パネルは既に説明してある。

通信メッセージ・フォーマット

メッセージの型式には、本質的には、端末装置１４から主データ処理システムへ送られることになる２つの異なる型式のメッセージとデータ処理システム１２から端末装置１４へ送られることになる４つの型式のメッセージとがある。端末装置から主データ処理システム１２へのメッセージは顧客が開始した取引のための通常第１の通信メッセージである取引要求メッセージ、並びにステータス・メッセージ（該メッセージは典型的には３つのメッセージ・シーケンス内の最後のメッセージ）を含む。ステータス・メッセージには２つの基本的な型式のステータス・メッセージがある。その第１のステータス・メッセージは通常の顧客る取引要求メッセージに対する通常の応答であり、要求された取引が完成される様式を端末装置１４に知らせる。コマンド・メッセージは端末装置14における論理状態を変え、又この変更を要求されない場合にはステータス・メッセージに対する問合わせコマンド・メッセージとして用いられるのがよい。初期設定ロード・メッセージは初期設定ロード・メッセージ（ＩＰＬ）のための例外ステータス・メッセージに応答して主データ処理システムから端末装置１４へ送られる。初期設定ロード・メッセージはメッセージ・テキスト、随意選択情報、フォント・テーブル、プログラム・ルーチン、並びに端末装置１４内のマイクロプロセッサ６０に動作的に接続されるデータ貯蔵装置（データ貯蔵モジュール）６６の揮発性ランダム・アクセス部分に貯えるためのデータ情報を含む。エコー・メッセージは首尾よい動作のための診断テストのために用いられ、端末装置１４が閉鎖状態にある間にのみ送られる。端末装置はエコー・メッセージに対してはエコー・メッセージで応答する。取引シーケンス内において第３の通信メッセージとしての地位を占め、顧客が要求した取引の完了若しくは取消を主データ処理システムへ知らせる返答ステータス・メッセージである。第２のステータス・メッセージは端末装置１４における通常の動作状態以外のステータス若しくは状態を示す例外ステータス・メッセージである。例えば、例外ステータス・メッセージは、サービス・ドアが開かれている状態において、主データ処理システムからの問合わせコマンドに対する返答として送られる。重大なエラー状態例えば顧客用ドアにおけるジャム又は端末装置の機構上の故障若しくは何らかの時間に関する初期状態の設定が検出されると、このステータス・メッセージが必要とされる。

主データ処理システム１２から端末装置１４へ送られる４型式のメッセージは取引返答メッセージ、コマンド・メッセージ、初期設定ロード・メッセージ、並びにエコー・メッセージを含む。取引返答メッセージは顧客による通常の取引における。

端末装置１４と主データ処理システム１２との間メッセージを送受するのに用いられる基本的なメッセージ・シーケンスには３つのメッセージ・シーケンスだけがある。単一メッセージ・シーケンスは端末装置１４から主データ処理システム１２へ転送される例外ステータス・メッセージから成る。例外ステータス・メッセージは異常状態が生じたということを示すか又は初期設定のための要求であつてもよい。主データ処理システムからのコマンド・メッセージは必要とされない。このメッセージの内容はその状態を示している。

２メッセージ・シーケンスは主データ処理システム１２から端末装置１４へのコマンド・メッセージ（初期設定ロード・メッセージ）及びこれに続いて端末装置１４から主データ処理システム１２へ送られる適切なステータス・メッセージ、又は主データ処理システムからのエコー・メッセージ及びこれに続く端末装置からのエコー・メッセージを含む。端末装置１４は端末装置が先行す

るコマンドを処理している間に受取られるコマンド・メッセージ、不適合メッセージ、又は要求されなかつた取引に対する取引返答メッセージは受取らない。いずれの場合においても、主データ処理システムは或る遠隔地のシステム又は直接に接続される近隔地のシステムであつてもよい。

どのような状態にあろうとも、端末装置14が初期的に受電状態にされる場合には、端末装置14が取引を受付けるように応答されうる前に端末装置14は初期設定ロード・メッセージを主データ処理システムへ要求して該メッセージを受取らなければならない。制御装置32へ接続される端末装置例えば第1図の端末装置36、44及び46はオフ・ライン・モードで動作してもよい。このような場合には、制御装置32は主データ処理システムとして働き、顧客による取引を例えば磁気テープ若しくは磁気ディスクに記録するように動作するのがよい。然る後に、取引情報は取引勘定を更新するように、後刻において取引勘定システムへ供給されるようになる。オン・ライン・モードで動作する場合には、主データ処理システムの或る種の機能例えば端末装置のための初期設定プログラムの貯蔵は制御装置32によつて処理されるのがよいが、すべての通信は通常、変更なしに主データ処理システム12との間で行われるのがよい。このようなオン・ラインの動作モードにおいては、主データ処理システム12はそのデータ・ベースに貯えられた勘定レコードを実時間即ち顧客が要求した取引が実行されるに従つて更新しうる。

端末装置14へ供給されている電力が失われる度毎にデータ貯蔵装置66のRAM部分の情報は消えるから、電力が供給されたときに初期設定が要求されなければならない。主データ処理システムからの初期設定情報を受取つた後、顧客による取引を受取るように端末装置14はその機能を再開されるのがよいが、それは主データ処理システムからのコマンドに従つて再開されるのがよい。初期設定は初期設定ロード・メッセージのための例外ステータス・メッセージを送らせるように単一メッセージ・フォーマットを使う端末装置14によつて達成される。然る後に、主データ処理システムは要求した初期設定情報を含む初期設定ロード・メッセージ（複数部分に分かれている。）を送ることによつて新しい通信シーケンスを開始する。初期設定情報を首尾よく受取ると、要求を出した端末装置14はステータス・メッセージを主データ処理システムへ送り返すことによつて2メッセージ・シーケンスを完了する。

あらゆるメッセージは端末装置14と主データ処理システム12との間で4バイトのヘツダ・フィールドから送り始められる。ヘツダ・フィールドのバイト1はメッセージ長さバイト（L）であり、該バイトはメッセージ・テキスト内のメッセージ・バイト数（Lを含む）の2進カウントを含む。バイト2は2進で表わされた1バイトの取引シーケンス番号（N）である。この番号は新しい顧客による取引毎に増分され、夫々の取引で交換されたあらゆるメッセージの中に含まれている。その番号は1から255までの範囲に亘る。顧客による取引に関係しないメッセージに対しては零（16進で00）が用いられる。従つて、新しい顧客による取引毎に増分される取引番号カウンタは16進のFFから16進の01へオーバーフローする。取引番号は短時間の停電後用い得るようにオペレータ用機能サブシステム76内の停電時情報保護用補助メモリに貯えられる。共通ヘツダ・バイトのバイト3はメッセージの型式従つて送られつつあるメッセージのフォーマットを同定するクラス・バイト(C)である。バイト4はヘツダ・フイールドの最後のバイトであり、メッセージ・クラス・バイトに対する修正バイトとして用いられるメッセージ・サブクラス（SC）を同定する。

メッセージ・クラス（C）及びメッセージ・サブクラス（SC）の取少ない可能な組合わせだけが実際に作られる。16進の01で表わされるクラスは端末装置14から主データ処理システムへ送られる取引要求メッセージを同定する。16進の01で表示されるクラスの中には9つのサブクラスが含まれている。ID番号が適正に送り込ま

れていないために顧客が要求した取引が首尾よく進行しないということを、１６進の０１で表わされるサブクラスは示している。１６進の０１で表わされるサブクラスは現金支払要求を表わしている。１６進の０２で表わされるサブクラスは取引勘定の問合わせを示している。１６進の０３で表わされるサブクラスは顧客が預金したいという要求を出しているということを示す。１６進の０４で表わされるサブクラスは顧客が預金を１つの取引勘定から他の取引勘定へ移したいという要求を出しているということを示している。16進の05で表わされているサブクラスは顧客が現金を端末装置に預けることによつて或るローン若しくはつけを支払いたいという要求を出しているということを示している。１６進の０６で表わされるサブクラスはキーボードの取引選択フイールド内の単一のキーを作動させるよりもむしろキーボードから予め決められた数を打込むことによつて取引の内容が同定される如き特殊の取引を示している。預金貯蔵所を被り預金フラップ(deposit flap)がこじあけられてしまつているために要求した取引が首尾よく進行しないということを、１６進の０７で表わされるサブクラスは示している。１６進の０８で表わされるサブクラスは預金を１つの取引勘定から他の取引勘定へ移すことによつてつけ若しくはローンを支払いたいという顧客の要求を示している。

１６進の１５で指定されるメッセージのクラスは端末装置１４から主データ装置システムへのステータス・メッセージを同定する。このクラスには５つのサブクラスのメッセージがある。１６進の０１で表わされるサブクラスは取引完了ステータス・メッセージを示している。１６進の０２で表わされるサブクラスはメッセージが或るコマンドの実行に応答し、そして共通ヘッダ・フイールド内のステータス数Ｎが零へセットされなければならないということを示している。１６進の０３で表わされるサブクラスは例外ステータス・メッセージがエラー状態を示しているか又は初期設定を要求し、そして取引番号Ｎは零へセットされなければならないことを示している。１６進の０４で表わされるサブクラスはステータス・メッセージが初期設定に応答し、そして取引番号が０へセットされなければならないということを示している。１６進の０８で表わされるサブクラスは回復要求メッセージ若しくはコマンド応答メッセージを表わすのに用いられ、そしてこのメッセージに対しては取引番号Ｎは０へセットされなければならないということを示している。回復要求メッセージは主データ処理システムが現時点での取引を首尾よく進めておらず、更新を必要とするということを示している。端末装置は例外ステータス・メッセージに応答する。

主データ処理システムから端末装置１４への取引応答メッセージは１６進の０Ｂで表わされるクラスによつて示される。このクラスにはサブクラス・バイトによつて示される９つのサブクラスがある。１６進の００で表わされるサブクラスはＩＤ番号が適正に送り込まれなかつたために取引が首尾よく進まないということを示している。16進の０１で表わされるサブクラスは現金支払取引要求を示している。１６進の０２で表わされるサブクラスは勘定問合わせ取引要求を示している。１６進の０３で表わされるサブクラスは預金取引要求を示している。１６進の０４で表わされるサブクラスは預金を或る取引勘定から他の取引勘定へ移したい場合の預金移動取引要求を示している。１６進の０５で表わされるサブクラスは端末装置に預けた預金を或る取引勘定へ移すことによつてローン若しくはつけを支払いたいという取引要求を示している。取引の内容が顧客用キーボード内の取引選択フイールド内の単一のキーの作動よりもむしろ数字キーボードから打込まれる番号によつて決定される如き特殊な随意選択取引を、１６進の０６で表わされるサブクラスは示している。端末装置１４の預金フラップがこじあけられてしまつているために首尾よく進まないところの顧客が要求した取引にメッセージが関係じているということを、１６進の０７で表わされるサブクラスが示している。預金を或る取引勘定から他の取引

勘定へ移すことによりローン若しくはつけを支払いたいという顧客の取引を示している。

１６進の０Ｃで表わされるクラスは主データ処理システムから端末装置１４へのコマンド・メッセージを同定する。コマンド・メッセージは特定の取引に関係していないから、ヘッダ・フイールドの取引番号Ｎは常に０へセットされている。16進の０１で表わされるサブクラスは取引開始コマンドを示している。１６進の０２で表わされるサブクラスは端末装置１４を閉鎖すべきコマンドを示している。１６進の０３で表わされるサブクラスは端末装置１４がコマンドに応答してどのような機能を遂行しないのがよいが、ステータス・メッセージに応答しなければならないという問合わせ型式のメッセージを示している。１６進の０４で表わされるサブクラスは伝送用暗号化用キーである第３のキー（キーＢ）をメッセージ内に含まれるキーに変えるためのコマンドを示す。１６進の０５で表わされるサブクラスは支援キー（キーＣ）を使つて転送されて来た暗号化用キー（キーＢ）をセットするためのコマンドを示す。１６進の０６で表わされるサブクラスは端末装置１４が初期プログラム・ロードを要求するように指揮されるということを示す。１６進の０７で表わされるサブクラスはメッセージが光学的表示を変えるためのコマンド又は取引書発行装置で印字されるべきメッセージを含むということを示している。１６進の０８で表わされるサブクラスは１６進の１５で表わされるクラスの中の１６進の０８で表わされるサブクラスで示す回復要求メッセージを主データ処理システムへ送る端末装置１４のためのコマンドを示している。

主データ処理システムから端末装置への初期プログラム・ロード・メッセージは１６進の０Ｄで表わされるクラスで指定され、このクラスには１６進の０１で指定されるただ１つのサブクラスがある。

主データ処理システムから端末装置１４へのエコー・メッセージは１６進の１０で表わされるクラスによつて指定される。このクラスには、４つのサブクラスのエコー・メッセージがある。１６進の００で表わされるサブクラスは基本エコー・メッセージを示し、単にエコー・メッセージを主データ処理システムへ返送するように端末装置を指揮するだけである。１６進の０１で表わされるサブクラスはビット・パターンをチエツクしてエコー・メッセージ化するエコー・メッセージ化コマンドを示している。エコー・メッセージ内のデータの諸バイトはすべての可能なビット・パターンを送つて通信施設の動作を検査するように設計されている。エコー・メッセージのパターンは転送されて来る２回目のエコー・メッセージのパターンと比較するため端末装置に保持される。１６進の０２で表わされるエコー・メッセージ可変レコード用サブクラスはエコー・メッセージが主データ処理システムで送り込まれたデータを含みうるということを除いて１６進の０１で表わされるサブクラスに類似している。端末装置はエコー・メッセージを送り返し、そしてそのエコー・メッセージは２回目の伝送されて来る同一のエコー・メッセージと比較するため貯えられる。伝送されて来る２回目のエコー・メッセージを受取ると、端末装置はエコー・メッセージに関するチエツクをし、サブクラス０１について説明したようにエコー・メッセージを発生する。エラー記録用データ要求メッセージは１６進の０３で表わされるサブクラスで指定される。このメッセージは端末装置から最新の８つのエラー記録レコードを送出させる。いずれのエコー・メッセージの伝送においても、どのような暗号化又は暗号解読化処理も施されない。

各々のメッセージ内の４バイトから成る共通ヘッダ・フイールドの後に、送られつつある特定のメッセージ型式に従つて決まるフォーマットのメッセージ・データが続く。端末装置１４から主データ処理システムへの取引要求メッセージについて言えば、共通ヘッダ・フイールドのバイト１乃至４の後に、３２ビットから成る暗号化されたフイールドを含むバイト５乃至８が続く。この３２ビットの暗号化されたフイールドはより詳細に後

述するが、概括的に言えばこのフィールドは顧客によりキーボードが打込まれ暗号化された型式の顧客ＩＤ番号及び現金カウンタ若しくは取引番号カウンタの内容であるのがよい変りうる１バイトの情報を含む。

バイト９は顧客用キーボードの預金引出選択フィールド内のどのキーが作動されたかということを示す預金引出選択（ＦＡＳ）バイトである。この９番目のバイトのデータ内容は顧客が要求した取引例えば預金を引出したい勘定形式を示す。１６進の２１は小切手勘定からの引出を示し、１６進の２２は貯金勘定からの引出を示し、１６進の２３はクレジット・カード勘定から引出を示し、そして１６進の２４は更に数的修正手段によつて定められる特別の随意選択勘定からの引出を示している。銀行との間で特別の諸定めを取交せば、顧客は複数の取引勘定の下に取引しうる。これらの取引勘定は予め決められた３デイジット（１０進）数で表わすことが出来る。キーボード上の特別の随意選択引出キーを作動させれば、上記予め取交された諸取引勘定の内の、顧客が欲している取引勘定が借方に記入されているかということを示すために顧客は３つまでの１０進数を数字キーボードから打込ませうる。これらの取引勘定の同定用数はバイト毎に１デイジットを付けて、複数のバイト１０－Ａ（但し、Ａはキーボードから打ち込まれる特別に定められた取引勘定番号が１、２、若しくは３を含むか否かに従つて値１０、１１、若しくは１２をとりうる）で転送される。ＦＡＳフィールドは可変長になりうるために、該フィールドは１６進でＦＥのデータ内容を有し諸可変長フィールドの夫々の限界を定めるのに用いられるフィールド分離（ＦＳ）バイトを後続させていなければならない。２つのＦＳバイトが隣接していると、フィールドの長さが零である、即ち、上記２つのＦＳバイト間にフィールドが入つていないということを示す。ＦＳバイトは該ＦＳバイトに先行するフィールドの終りを定める。

顧客用キーボードの預金選択フィールド内の作動されたキーによつて指定される預金選択（ＴＡＳ）フィールドは預金引出選択（ＦＡＳ）フィールドのためのＦＳバイトをその後に置いている。１６進の３１は資金を小切手勘定に預けたいということを示し、１６進の３２は資金を貯金勘定に預けたいということを示し、１６進の３３は資金をクレジット・カード勘定に預けたいことを示し、そして１６進の３４は最初のＴＡＳバイトに直続する３つまでのデイジットによつて変えられうる特別の随意選択預金勘定へ預けたいということを示す。これらの数字修正手段はＴＡＳフィールドにおいてＦＡＳフィールドと同じ意味を有する。ＴＡＳフィールドは可変長であるために、該フィールドは又１６進のＦＥデータ内容を有するフィールド（ＦＳ）バイトを後続させていなければならない。預金選択フィールドのためのＦＳバイトに続いて、クレジット・カード上の磁気記録条帯から既取られるデータが転送される。アメリカ合衆国の銀行協会で定めている標準コードからパリテイ・ビットを除けば、メッセージの各々のバイトの中にクレジット・カードからのデータ内の４ビットから成る２文字を置くことが可能になる。クレジット・カードの磁気記録条帯に奇数の文字が記録されている場合には、該メッセージのすべてのバイトを満たすようにメッセージの最後バイトは１６進のＦで満たされる。クレジット・カード・データ開始文字、クレジット・カード・データ終了文字、及び長さ方向冗長性検査（ＬＲＣ）文字は伝送される取引要求メッセージから除かれるが、これらの文字は端末装置１４でチエックされている。

端末装置１４から主データ処理システムへ伝送されるステータス・メッセージはメッセージのためのメッセージ長さ（ｋ）　取引番号（Ｎ）、メッセージ・クラス（Ｃ）、及びメッセージ・サブクラス（ＳＣ）を同定する４バイトの共通ヘッダ・フィールドで始まる。バイト位置５乃至８は３２ビットの暗号化されたフィールドを形成している。この３２ビット・フィールドはより詳細に後述するが、概括的に言えば、８ビットで表わされる取引番号（Ｎ）、額面金額のための循回する

現金カウント２（ＣＮＴＲ２）を表わす８ビット、ステータス・バイト数を表わす８ビット（ＣＢ）、及び額面金額のための循回する現金カウント１（ＣＮＴＲ１）を含む。バイトＣＢは通常のステータス・メッセージのための、メッセージの暗号化された部分（バイト５乃至８）に続くステータス兼問合わせデータ・バイトの数を２進カウントで表わす１バイト・フイールドである。回復要求メッセージに対しては、このＣＢフイールドは最後の取引要求メッセージに対する取引応答メッセージからの"アクション・フイールド"を入れる。このアクション・フイールドは取引返答メッセージの中の３２ビットの暗号化されたフイールドの一部として伝送される８ビット・フイールドである。この３２ビットの暗号化されたフイールドの２つの８ビット・カウンタ部分（ＣＮＴＲ）は第２及び第１の現金支払機構によつて発行された請求書数の２進カウントを示す。これらの請求書数は発行される請求書毎に増分され、１６進のＦＦから１６進の００へ移る諸カウンタ部から取出されると。上記の２進カウントはこのカウントが短時間の停電の間保存されるようにオペレータ用機能サブシステム７６の補助メモリに貯えられる。バイト５乃至８の３２ビットの暗号化されたフイールドに続いて、データ・フイールドがある。このデータ・フイールドはバイト位置９乃至１２に置かれる４バイトのステータス・フイールドである。これらの４バイトは後述するように端末装置１４の各時点でのステータスを表わしている。大部分のステータス・メッセージはバイト位置１３に置かれるＦＳバイトで終る。しかしながら、問合わせコマンド・メッセージに応答して送られるステータス・メッセージはサブシステム７６の補助メモリに貯えられる１２８のバイトの内の１１２バイトを含み、これらのバイトは４つのステータス・バイトに続いて転送される。このステータス・メッセージに対してはフイールドＣＢは数１１６を含む。問合わせメッセージに応答しては送られない非揮発性メモリの１６バイトは８バイトから成る２つの暗号化用キーを含む。ステータス・メッセージが回復要求メッセージに応答して再送されつつないならば、４つのステータス・バイトは最後の取引ステータス・メッセージの４バイトを含み、元の完全な取引要求メッセージによつて続けられる。然る後に、この情報は主データ処理システムをして回復を要求させた事象に先立つて存在した諸状態を、主データ処理システムをして再構成させる。

ステータス・メッセージのバイト位置９乃至１２に置かれる４つのステータス・バイトの中の３２ビットの位置の各々には予め決められた意味を有する。これらの意味は主データ処理システムが各々の端末装置１４の夫々の動作をアクセスし制御するのに十分なだけの詳しさで端末装置１４の物理的な動作上のステータスを定めるように割当てられている。これらの意味は以下に表の形式で説明されており、この表において左側の番号は０から３までのステータス・バイト番号を示しており、そしてステータス・バイト０はステータス・メッセージのバイト位置９にあり、ステータス・バイト３はステータス・メッセージのバイト位置１２にある。各々のステータス・バイトはビット０乃至ビット７で指定される８ビットから成り、ビット０は最高位ビット位置にあり、ビット７は最低位ビット位置にある。

バイト	ビット	説　明
0	0	取引完了ステータス・ビット。このビットは各々の取引の開始時に論理的な１へセットされ、この論理的な１は取引が完了しておらず、取引応答メッセージが必要とされるということを示す。
0	1	取引応答メッセージ内の取引シーケンス番号無効ビット。このビット位置は新しい取引が開始される度毎に論理的な０へリセットされる。データ処理システムから受信されるメッセージの

共通ヘッダ・フィールド内の取引番号が正しくないときはいつでもこのビット位置は論理的な1へセットされる。ヘッダ・フィールドの取引番号位置に関して意味のある情報を伝送しないエコー・メッセージについては例外である。

2　取引応答メッセージ内の取引サブクラス無効ビット。このビット位置は新しい取引が開始される度毎に論理的な0へリセットされ、そして共通ヘッダ・フィールドの第4バイト即ちサブクラス・バイトの番号が取引要求メッセージのそれとは異なる取引応答メッセージが受け取られるときはいつでも、論理的な1へセットされる。バイト0のビット0はこのビット位置と同時

れたフィールド内の金高表示バイトが正しくない金高を示す取引応答メッセージが受取られるときにはいつでも、論理的な1へセットされる。バイト0のビット0（ＡＭＴ）はこのビット位置が論理的な1へセットされるときにはいつでも、論理的な1へセットされる。

5　割り当てられず。

6　顧客取引取消ビット。このビット位置は各々の新しい取引の開始時に論理的な0へリセットされ、そして取引要求メッセージの伝送に続いて顧客が顧客用キーボード上の取消キーを押した場合には、論理的な1へセットされる。

7　顧客用時間超過ビット。このビット位置は各々の顧客取引開始

にセットされねばならない。

0　3　クラス無効ビット。このビット位置は例外ステータス・メッセージが送られた後0へリセットされ、そして共通ヘッダ・フィールドのバイト3にクラス無効表示を含むメッセージが主データ処理システムから送られて来たときにはいつでも、論理的な1へセットされる。例えば、端末装置14が要求しなかつた初期設定（ＩＰＬ）メッセージ又は要求しなかつた取引に対し取引応答メッセージを受取ることがある。

0　4　取引応答メッセージ内の金高誤りビット。このビット位置は各々の新しい取引の開始時に論理的な0へリセットされ、そして取引応答メッセージの暗号化さ

時に論理的な0へリセットされ、そして顧客用キーボードから番号を打込むのに、又は預金フラップを経て預金を入れるのに顧客が予め設定されている時間期間よりも長い時間を要したときにはいつでも、論理的な1へセットされる。このビット位置若しくはビット位置06が論理的な1へセットされるときにはいつでもバイト0のビット0は論理的な1へセットされなければならない。

1　0　コマンド不受理ビット。このビット位置はコマンド・ステータス・メッセージが送られた後論理的な0へリセットされ、そしてコマンドが受取られる時刻には端末装置がビジーにあるため実行され得ないコマンド・メッ

セージの受付時に、論理的な1へセットされる。

コマンド無効ビット。このビット位置はコマンド・ステータス・メッセージの送出時に論理的な0へセットされ、そしてコマンド・メッセージの中の幾つかのフイールドがなくなつているコマンド・メッセージが受取られるときにはいつでも、論理的な1へセットされる。このようなコマンド・メッセージは例えば、新しいキーを含まないキー変更コマンド又は新しい表示フイールドのない表示変更コマンドである。このビット位置は又共通ヘッダ・フイールドのバイト4に無効サブクラス表示を含むコマンド・メッセージに応答して論理的な1へセットされる。

1 2 IPL要求ビット。このビット位置は主データ処理システムからの初期設定ロード・メッセージを適正に受取つたとき論理的な0へリセットされ、そしてオペレータ若しくは顧客施設保守員用アクセス・パネルの閉鎖又は主データ処理システムからのコマンドに対する応答時に端末装置14は閉鎖状態から営業状態へ移る度毎に論理的な1へセットされる。このビットは又、端末装置14が該装置を指揮してIPLを要求するコマンド・メッセージを受取る度毎に、論理的な1へセットされる。

1 3 IPL兼処理ビット。このビット位置はバイト1のビット位置2と組になつて修正ビットとして作用する。00に等しいビット2及びビット3の組合わせは端末装置が初期設定されているということを示す。この状態は端末装置が営業状態にあるときにのみ生ずる。10に等しいビット2及びビット3の組合わせは初期設定のための要求を出したが、初期設定ロード・メッセージがまだ受取られていないということを示す。11に等しいビット2及びビット3の組合わせは初期設定ロードが進行中であるということを示す。

1 5 Cフイールド及びSCフイールド・エラー・ビット。このビット位置は例外ステータス・メッセージの送出時に論理的な0へリセットされる。主データ処理システムから伝送されて来たコマンド・メッセージの暗号化されたデータ・フイールド内のク

4 現金カウンタ・ビット。このビット位置は新しい顧客取引の開始毎に論理的な0へリセットされる。受取られた取引応答メッセージの暗号化されたフイールド内の現金カウンタ・バイト（CNTR）の内容と端末装置内の現金カウンタの内容とが一致しないときにはいつでも、このビット位置は論理的な1へセットされる。現金カウンタは新しい勘定書が発行される度毎に増分される最大値から最小値へ移る型式のカウンタ（ロールオーバ・カウンタ）である。このビット位置が論理的な1へセットされる度毎に、バイト0のビット0は論理的な1へセットされなければならない。

ラス（Ｃ）バイト及びサブクラス（ＳＣ）バイトが共通ヘッダ・フイールドのクラス・バイト及びサブクラス・バイトと一致しないとき、このビット位置は論理的な１へセットされる。この不一致は暗号化用キーに関しての不一致エラー若しくは主データ処理システムにおけるエラーが生じているということを示す。通常のコマンド・メッセージにおいては、共通ヘッダ・フイールドのクラス（Ｃ）バイト及びサブクラス（ＳＣ）バイトは（各々のバイトの始めの方の４つの０ビットを感知することによつて１つにまとめられて）単一のクラス及びサブクラス（Ｃ及びＳＣ）バイトになるように結合される。

1	6	取引要求－取引応答シーケンス中の通信時間超過表示ビット。このビット位置は、新しい顧客取引の開始毎に論理的な０へリセットされ、そして取引要求メッセージの送出に続いてこれに対応する取引応答メッセージを受取るまでの間に予め決められた時間が経過したときにはいつでも、論理的な１へセットされる。このビット位置が論理的な１へセットされるときにはいつでもバイト０のビット０は論理的な１へセットされねばならない。
1	7	不適合メッセージ・ビット。このビット位置は例外ステータス・メッセージを送つた後に論理的な０へリセットされる。要求した予め決められたメッセージ・フォーマットに対応しないメッセージが受取られるときにはいつでも不適合メッセージの表示を与えるために、このビット位置は論理的な１へセットされる。例えば、バイト数が共通ヘッダ・フイールド内のメッセージ長（Ｌ）表示に一致しないとか、データ・バイトを読取つた場合にパリテイ・エラーが生じたとか、又はバイト位置に無効なデータが含まれている場合である。
2	1	カード保持ビット。このビットは新しい顧客取引の開始毎に論理的な０へリセットされ、そして顧客によつて端末装置内に挿入されたクレジット・カードを端末装置１４が保持する状態で顧客が要求した取引が終了されるときにはいつでも、論理的な１へセットされる。主データ処理システムからのコマンドに応答しての結果としてよりも端末装置１４でのハードウエア・エラーの結果としてカードが保持されているということを、このビット位置は示す。
		取引書発行中エラー発生ビット。このビット位置は新しい顧客取引の開始毎に論理的な０へリセットされ、そして取引書例えば請求書若しくは取引計算書の発行中にエラーが生ずるときにはいつでも、論理的な１へセットされる。このビット位置は、取引書が保管領域から保持所へ運ばれるときにはいつでも、論理的な１へセットされる。再施行のときに取引が完全になされう

ることがあるから、このビット位置は不完全な顧客取引を必ずしも示していない。

22 貯蔵所回復不可能エラー・ビット。このビットは新しい顧客取引の開始毎に論理的な0へリセットされ、そしてエラー状態例えばジャムが端末装置の貯蔵所で生じ、該端末装置が上記エラー状態から回復し得ないときにはいつでも、論理的な1へセットされる。

23 表示テーブル・オバーフロー・ビット。このビットはステータス・メッセージの伝送時に論理的な0へリセットされ、そして主データ処理システムから受取られる表示変更コマンド・メッセージが端末装置の表示装置が処理しうるよりも多くの表示データを含むとき、論理的な1へセットされる。不適当な表示メッセージは端末装置14によつては受取られない。

24 割当てられず。

25 割当てられず。

26 割当てられず。介入必要ビット。このビットは介入の必要性が生じたときセットされ、そして介入必要インデイケータがオフにされるときリセットされる。

27 カード取出時間超過表示ビット。このビットは新しい顧客取引の開始時に論理的な0へリセットされ、そして端末装置からクレジット・カードを取出すことなしに顧客がクレジット・カードを取出しうるようになつてから予め時間が経過したときにはいつでも、論理的な1へセットされる。このビットは或る種の介入を必要とするということを示す。通常、主データ処理システムは端末装置にクレジット・カードを保持させることによつて応答する。

30 開業／閉鎖ビット。このビットは端末装置が開業し、顧客の取引要求を受付けうる状態になるときにはいつでも、論理的な0へリセットされ、そして端末装置が閉鎖するとき論理的な1へセットされる。

31 現金不足状態ビット。このビットは新しい顧客取引の開始毎にリセットされる。このビットは最高額の現金を支払いうるに十分な現金が端末装置にあるか否かを示すハードウエア・スイッチに応答する。ステータス・メッセージが応答する先行の現金支払取引の実行中に現金不足状態が生ずるときにはいつでも、このビットは論理的な1へセットされる。このビットがセットされると、介入が必要とされるということが表示され、端末装置は閉鎖される。

32 支援暗号化用キー無効ビット。このビットはステータス・メッセージの伝送時に論理的な1へリセットされ、そして主データ処理システムから不適正な暗号化用キー（すべて零を含むキー）を含むキー変更型のコマンド・メッセージを受取るとき、論理的な1へセットされる。

33 最終取引発行ビット。このビットは新しい顧客取引の開始時に論理的な0へリセットされ、そ

してステータス・メッセージが応答する先行の最後の取引中に利用しうる最後の取引書が発行されたということを取引書感知器が示すとき、論理的な１へセットされる。

3　4　預金フラップ（ドア）若しくは支払ゲート開放持続表示ビット。このビットはステータス・メッセージの伝送時にリセットされ、そして閉じられねばならない場合に預金フラップ若しくは支払ゲートが開放されたままにあるときに論理的な１へセットされ、フラップ若しくはゲートが正常な動作をしていないということを示す。

3　5　回復不可能なハードウエア故障ビット。このビットは例外ステータス・メッセージが送られた後論理的な０へリセットされ、そして、取引の実行中又は他の任意の時刻に正され得ないジャム若しくは他のエラー状態が生じたときにはいつでも、論理的な１へセットされる。このビットがセットされると、介入が必要とされ、端末装置は閉鎖されるということを表示する。

3　6　顧客用ドア開放持続ビット。このビットはステータス・メッセージの伝送時に論理的な０へリセットされ、そして閉じられているべきときに顧客用キーボード及び表示装置へのアクセスを与える顧客用ドアが開放されているとき、論理的な１へセットされ、ドアが正常に動作していないということを示す。このビットがセットされると、介入が必要とされているということを示し、端末装置を閉鎖する。

3　7　安全性確保インターロック・ビット。このビットはオペレータ・アクセス用ドアが閉じられているとき論理的な０へリセットされ、そして上記ドアが開かれているとき論理的な１へセットされる。このビットが論理的な１へセットされるとき端末装置１４は閉鎖される。

主データ処理システム１２から端末装置１４への取引応答メッセージは取引要求メッセージに応答して発生される。取引応答メッセージは全メッセージ長（Ｌ）、取引番号（Ｎ）、メッセージ・クラス（Ｃ）、及びメッセージ・サブクラス（ＳＣ）を指定する標準の４バイト共通ヘッダ・フィールドから始まる。共通ヘッダ・フィールドを構成する４バイトに続いて、４バイト（３２ビット）の暗号化された情報、可変長随意表示データ・フィールド、フィールド分離文字（ＦＳ）、可変長随意取引書印字フィールド、及びフィールド終了分離文字（ＦＳ）が続く。４バイトの暗号化されたフィールドは1バイトの現金カウンタ２の数（ＣＮＴＲ２）、１つのアクション・バイト、１バイトの現金カウンタ１の数（ＣＮＴＲ１）、並びに取引応答メッセージが支払いを認めている取引書数を指定する数量バイト（ＡＭＴ）を含む。端末装置は要求に対して許された量を調べる。

アクション・バイトは顧客取引のデータ内容と両立する様式で顧客取引を完成させるように端末装置１４を指揮する主データ処理システムからの１バイトの命令である。

ビット０。ビット０が論理的な１へセットされると、暗号化されたフィールドに直続する随意表示データ・フィールドによつて指定される標準の端末装置用表示メッセージを直ちに表示するように、端末装置１４は制御される。０乃至１２７によつて指定される１２８までの夫々のメッセージはマイクロプロセッサ６０に関連付けられるデー

タ貯蔵装置６６に貯えられる。アクション・バイトのビット０が論理的な１へセットされると、取引応答メッセージのバイト位置９での１バイトの随意表示フイールドの２進値によつて指定されるところの上記１２８のメッセージの内の１つを表示するように、端末装置１４は制御される。

ビット１。ビット１が論理的な１になると、暗号化されたフイールドに直続する随意表示データ・フイールドに置かれた随意表示メッセージを直ちに表示するように、端末装置１４は制御される。ビット１が論理的な１へセットされると、随意表示データ・フイールドの始めのバイト９は、バイト９を除いて表示メッセージの長さをバイト数で示す２進数を含む。バイト９に直続して、取引応答メッセージは、各々のバイトが１つの表示文字を表示する状態で、ＥＢＣＤＩＣコード方式で所望の表示メッセージのテキストを含む。

ビット２。アクション・バイトのビット位置２の論理的な１は端末装置１４が情報を取引書に印字するように制御され、且つ取引応答メッセージの取引　印字データ・フイールドはＥＢＣＤＩＣコードで印字されるべきデータを含むということを示す。

ビット３。用いられず。

ビット４。ビット４の論理的な１は要求された顧客取引が受入れられたということを示す。

ビット５。ビット５の論理的な１は顧客のクレジット・カードが端末装置１４に保持されるべきであるということを示し、その論理的な０はクレジット・カードが顧客に返却されるべきであることを示す。

ビット６。このビットの論理的な１は端末装置１４が取引の実行に進む前に顧客がその取引を受認するかどうかということが要求されていることを示す。キーボードの制御フイールドの取消キー又は進行キーを押すことによつて顧客はその取引を受認するかどうかについて応答する。典型的には、顧客がキーを選択するとその取引の或る内容が表示される。例えば、メッセージ"ＴＲＡＮＳＦＥＲ　$５０.００　ＦＲＯＭ　ＳＡＶＩＮＧＳ　ＡＣＣＯＵＮＴ　ＴＯ　ＣＨＥＣＫＩＮＧ　ＡＣＣＯＵＮＴ－ｄｅｐｒｅｓｓ　ｃａｎｃｅｌ　ｏｒ　ｐｒｏｃｅｅｄ"が表示される。

ビット７。用いられず。

取引応答メッセージの終りでの取引書印字フイールドは２枚までの取引書のための印字データを送るための複数のサブフイールドに分けられている。第１のサブフイールドは情報例えば両取引書に同じである顧客名及び勘定番号を送る共通データ・フイールドである。共通データ・フイールドは端末装置１４の貯蔵装置６６に貯えられた印字メッセージを印字するように端末装置を制御するか又は共通データ・フイールドの一部として標準のＥＢＣＤＩＣコードで伝送されるメッセージを印字するように端末装置を制御する。共通データ・フイールドの第１バイトは印字データ源を決定する。このバイトが１乃至１２７（１６進で８０以下）の数を含むならば、印字データは上記第１バイトに直続する共通データ・サブフイールドに標準のＥＢＣＤＩＣコードで貯えられている。この場合には、第１バイトは２進の長さカウントを表わし、この長さバイトを除いて共通データ・フイールド内のバイト数を示す。共通印字データが印字メッセージによつて与えられる場合には、特定の印字メッセージを同定する印字メッセージＩＤ番号が共通データ・サブフイールドの第１であつて１つのバイトとして１２８（１６進の８０）へ加えられ伝送される。例えば、共通データが印字メッセージ番号３０から取られる場合には、１バイトの共通データ・サブフイールドは２進で表わされた番号３０＋１２８＝１５８（１６進で９Ｆ）を含む。ＩＤ番号０に対応する１バイトのデータ内容は共通データ及び取引書データのための境界決定バイトとして用いられ、メッセージ０を印字メッセージとして定義するのには用いられない。取引書番号１データ・サブフイールドは共通データ・サブフイールドの後の境界決定バイト（１６進で８０）に直続する。取引書番号１データ・サブフイールドは実際のＥＢＣＤＩＣコードの印字メッセージを送つてもよいし又は記録された印字メッセージを同定してもよいが、共通データ・フイ

ールドと同じフォーマットを使用する。しかしながら、取引書番号1データ・サブフィールドによつて制御される印字情報は取引書フォーム1によつて指定されるフォーム1の上にのみ印字される。境界決定文字（16進で80）は取引書番号1データ・サブフィールドに直続する。取引書番号2データ・サブフィールドは第2の境界決定文字に直続する。取引番号2データ・サブフィールドは共通データ・サブフィールド及び取引書番号1データ・サブフィールドと類似のフォーマット及びデータ内容を有する。取引書番号2データ・サブフィールドはEBCDICコードで伝送される印字メッセージを含んでもよいし又は記録された印字メッセージを同定してもよい。取引書番号2データ・サブフィールドが存在しない即ち0バイトの長さを有するならば、第2の取引書フォームは印字されないか又は発行されない。フィールド分離（FS）文字は取引書番号2データ・サブフィールドに直続して取引書印字フィールドの終り及び取引応答メッセージの終りを告げる。取引書フォームの印字は英語で読める共通のフォーマットで、左上コーナで始まり、左から右へ進みそして1行ずつ下方へ進む。EBCDICコードのキャリッジ制御コードは取引書の1行の印字を終らせ、そして取引書に印字すべき次の文字を1行下の行の最左端の文字位置に印字する制御のために用いられる。印字動作は共通のテキストが先ず取引書フォーム1の上に印字され、取引書1テキストが取引書フォーム1の上に印字され、共通テキストが取引書フォーム2の上に印字され、そして最後に取引書2テキストが取引書フォーム2の上に印字されるという予め決められたシーケンスで進む。

コマンド・メッセージは主データ処理システム12から端末装置14へ送られ、コマンド・メッセージのデータ内容に従つて端末装置の動作若しくはステータスを制御する。各々のコマンド・メッセージはメッセージ長（L）、取引番号（N）、メッセージ・クラス（C）及びメッセージ・サブクラス（SC）を含む4バイト長の共通ヘッダ・フィールドで始まる。4バイト長の暗号化されたフィールドが4バイト長のヘッダ・フィールドに続く。4バイト長の暗号化されたフィールドは第1現金カウンタ・バイト（CNTR1）、単一バイトの中に結合されたクラス表示及びサブクラス表示を含むクラス及びサブクラス・バイト（CNSC）、第2現金カウンタ・バイト（CNTR2）、並びに特殊バイト（SPEC）を含む。特殊バイトはコマンドを与えられた端末装置から主データ処理システムへのステータス応答メッセージによつて供給される情報を示すために問合わせ形のコマンド・メッセージに用いられる。特殊バイトのビット0乃至4は割当てられず、通常、論理的な0として転送される。ビット5は端末装置がその最後のステータス・メッセージを再送するように制御されつつあるということを示すために論理的な1へセットされる。端末装置が現時点のステータス・メッセージ並びにオペレータ用機能サブシステム76内の補助貯蔵装置に貯えられている112バイト（2つの暗号化用キーを含まず）を転送しなければならないということを示すために、ビット6は論理的な1へセットされる。特殊バイトのビット7の論理的な1は端末装置が通常のステータス・メッセージを転送するように制御されるということを示す。ビット5、6、及び7は相互に排他的であり、一時にはただ1つのビットのみがセットされる。

随意に暗号化される2つのフィールドがコマンド・メッセージの共通ヘッダ・フィールド及び4バイト長の暗号化されたフィールドに続く。随意に暗号化される第1のフィールドは8バイト長の暗号化用キーの第1の半分を運び、随意に暗号化される第2のフィールドは8バイト長の暗号化用キーの第2の半分を運ぶ。これらの第1及び第2の、随意に暗号化されるフィールドはキー・セット・コマンド又はキー変更キーに続いてのみ含まれる。第3の即ち伝送用の暗号化用キー（キーB）でコマンド・メッセージを暗号解読化し、然る後に将来のすべての通信のために第1及び第2の、随意に暗号化されたフィールドで伝送されて来たキーを置き換えることによつて端末装置14はキ

一変更コマンドに応答する。キー・セット・コマンドは新しいキーが補助貯蔵装置に貯えられている支援キー（キーＣ）で暗号化されるということを除いて、キー変更コマンドと同様に動作する。表示変更形コマンド・メッセージにおいては、随意に暗号化される２つのフイールドはメッセージの中には含まれないが、クリア・テキスト随意データ・フイールドは４バイト長の暗号化されたフイールドに続く。クリア・テキスト随意データ・フイールドは標準のＥＢＣＤＩＣコードのインデックス番号（ＩＮＤＸ）（これに続くデータ・フイールド長バイト（ＬＤ）及び新しい表示テキスト）で始まる。表示変更メッセージ形のコマンド・メッセージは顧客によつて眺められる実際の表示に影響を与えるのではなく、その代りにデータ貯蔵装置６６に貯えられた表示メッセージのデータ内容を修正する。例えば、表示メッセージＩＤ番号４０を有する貯えられた表示メッセージ"take out credit card"をメッセージ"remove credit card"へ変えたいものとする。インデックス・バイト（ＩＮＤＸ）は貯えられたメッセージの、変更しようとする表示メッセージＩＤ番号を含む。データ・フイールド長バイト（ＬＤ）は直続する新しいメッセージのテキスト内のバイト数を示す２進数を含む。新しいメッセージがデータ貯蔵装置６６内の各々の表示メッセージを入れておくテーブルに入れられうるバイト数にぴつたり合うのにはあまりにも長い場合には、そのコマンドは実行されず、これに続くステータス・メッセージが、そのコマンドが実行されなかつたということを示す。表示メッセージの各々が可変長であり、主データ処理システムから端末装置１４へのすべてのメッセージが偶数のバイトを含むことが必要である場合には、表示テキスト（表示メッセージ）の終りに全体として偶数になるだけの任意数の文字を付加する必要がある。この付加される文字数はデータ・フイールド長バイト（ＬＤ）ではカウントされないが、コマンド・メッセージの共通ヘツダ・フイールドの中のメッセージ全長フイールド（Ｌ）でカウントされる。

初期設定ロード・メッセージは停電時に失われてしまうことがあるデータ貯蔵装置６６のランダム・アクセス・メモリ部分のための情報を与える。該メッセージは又端末装置を随意に新しく改めて初期設定するのに用いられてもよい。上記メッセージは後続するデータ・フイールド内のバイト数を指定する２バイト長２進数フイールドを後に置いている４バイト長の共通ヘツダ・フイールドで始まる。上記のデータ・フイールドは初期設定ロード・メッセージの最後のフイールドとなり、データ貯蔵装置６６に貯えられる情報に対応する内容（顧客毎の像情報）を含む。データ・フイールド内の重要な情報例えばマイクロ・プログラム・ルーチン及び随意選択バイトは４バイト長のシーケンシヤルなセグメントで表わされる第３の転送キー（キーＢ）で暗号化される。

概括的に言えば、初期設定中に受取られる顧客毎の像情報は端末装置毎に変りうる情報を提供し、それ故読取専用メモリでは容易には実施され得ない。メッセージ１乃至４９で指定される４９までの予め決められたメッセージを含みうるところの貯えられた顧客の表示メッセージ及び印字メッセージは顧客毎の像情報の中に含まれる。又、所与の端末装置例えば銀行の顧客によつて選択されている非標準的な文字若しくは図形を表示しうる５７４までのバイトを含む随意選択フォント・テーブルがメッセージ５０として含まれている。所与の端末装置で施行されている利用可能な諸随意選択事項の特定の組合わせを保つておくために要する或る量のプログラミング情報及びプログラム制御情報が顧客毎の像情報の中に含まれている。

取引メッセージの組立て

次に、参照する第３図乃至第５図のブロック・ダイヤグラムには、顧客が要求した取引の実行中に主データ処理システム１２と端末装置１４との間でやり取りされる通信がより詳細に例示されている。本発明の動作を理解し易くするために、通信システムの動作を顧客による取引の特定の例を用いて説明する。しかしながら、端末装置は顧客

が要求する多数の取引の内の任意の１つの取引を遂行し得、これらの特定の取引例に制限されるものではないということは認められよう。

特定の例として、端末装置１４は銀行の支店での階段昇降式ステーションを提供する仕切り壁に窓口を設けた型式の端末装置であるものとする。この端末装置は端末装置４６（第１図）と類似の方式で閉ループ、制御装置３２、そして該制御装置を経て主データ処理システム１２へ接続されるものとする。端末装置４６は顧客通信施設を銀行の外に置き端末装置の大部分を銀行の内部に置くようにして銀行の支店の外壁を通して延びている。オペレータ保守用アクセス・パネルは銀行の支店の内部のサービス・ドアを経てアクセスしうる。潜在的な顧客が端末装置４６に近づくとき、端末装置のキーボード領域の照明及びキーボード上の信号灯はその端末装置が利用しうる（開業）状態にあることを示す。ライトが点灯されておらず、表示装置が閉鎖状態にあることは、端末装置が閉鎖状態にあり取引の実行にはその端末装置が利用し得ず、どのような顧客による動作も無視されるということを示す。端末装置が営業状態にあるならば、取引のある顧客は自分のクレジット・カードをスロットへ挿入することによつて取引を開始する。説明しようとする例においては、顧客が資金を自分の貯金勘定から小切手勘定へ移したい場合を仮定する。

1.取引要求メッセージ

顧客による取引のための３つの部分から成る通信シーケンスの第１の部分が第３図に例示されている。端末装置のマイクロプロセッサ６０は物理的若しくは機能的ブロックとの特定の接続なしに第３図では概括的にのみ示されている。第２図に示されるような論理的な相互接続がなされ、又動作に関する制御及びデータ処理がマイクロプロセッサ６０によつて遂行されるということは認められよう。

これから取引をしようとする顧客がクレジット・カード１００を銀行から手渡されるときに、その顧客は６デイジットの顧客同定（ＩＤ）番号を割当てられる。この顧客ＩＤ番号はクレジット・カード１００上の磁気記録帯上に記録される情報に随意に関係付けられるのがよい。クレジット・カード１００が端末装置４６へ挿入されると、そのクレジット・カードの存在が感知され、クレジット・カード移送機構がそのクレジット・カードを端末装置の中へ引込み、クレジット・カードの適正な配置及びステータスを感知する読取ヘッドを通過される。クレジット・カードが適正に配置されていないならば理解し得ないデータ又は端末装置４６によつては受入れられ得ない型式のデータを含むことになり、クレジット・カードは返却される。（もしクレジット・カードが満期になつているならば、そのことは主データ処理システムのコマンドに保持されるのがよい。）適正なクレジット・カードであるとするならば、クレジット・カード１００はカード読取機構１０２を通過され、そこにおいて磁気記録帯上の情報が読取られ、読取られた情報はデータ貯蔵装置６６のランダム・アクセス・メモリに貯えられ、そしてクレジット・カードはカード保管保持領域に置かれる。クレジット・カード１００は米国銀行協会によつて決められている標準のクレジット・カードと互換性を有する。このことは磁気記録帯が一連の５ビット・ワード（パリテイ・ビット及び４つのデータ・ビットから成るワード）を含むということを意味する。４つのデータ・ビットはカード開始（ＳＯＣ）文字、フイールド分離文字、及びカード終了（ＥＯＣ）文字を含む。数字は２進化１０進方式で表わされる。磁気記録帯の代表的なフオーマツトはカード開始（ＳＯＣ）文字で始まり、該文字に続いて１９までの文字から成る勘定番号、フイールド分離文字、クレジット・カード満期日の月及び年を指定する４文字、任意データ・フイールド、カード終了（ＥＯＣ）文字及び長さ方向冗長検査文字がある。磁気記録帯に記録されうる最大の５ビット文字数は４０である。諸文字が読取られるとき、初期設定用随意選択事項として与えられる選択キー（Ｋ１）は磁気記録帯からのシーケンシヤルな８つの文字を選択するための開始点を決定する。例

えば、Ｋ１が数５を含むならば、メッセージ開始（ＳＯＭ）に続く第５番目から第１３番目の文字がステップ１０４でそれらのパリテイ・ビットなしに選択されて３２ビットを形成する。これらの３２ビットは暗号化アルゴリズム１０６で処理されて３２ビットから成る暗号化されたデータを発生する。

顧客ＩＤ番号の一部又は全部とこれに対応するクレジット・カード情報との比較は初期設定時に指示される顧客随意選択事項として選択的になされるのがよい。この比較が随意選択事項として選ばれないならば、ＩＤ番号とクレジット・カード情報との間の対応は無差別に選択されるのがよい。しかしながら、端末装置１４が主データ処理システムとオフ・ラインの制御の下で動作する場合には、上記の対応の有無に関する比較は実行することが不可能である。端末装置内のみでのチエック用随意選択事項が選択されるならば、２つのキーがそのチエックが実行される方式を指定する。

第１のチエック・キー Ｋ１はクレジット・カードから読取られる連続した８文字から成る任意のグループを選択する。キーＫ１はＳＯＭに続く８文字の内の第１の文字の位置を指定する。８文字は常にそうではないが、クレジット・カードの勘定番号フイールド内に完全に入つているように選ばれる。この例としてＫ１が５として選ばれるならば、文字５乃至１３が選ばれる。

第２のチエック・キーＫ２はそのチエックが開始されんとするデイジット位置を指定することによつて顧客ＩＤ番号内のどれだけのデイジット数がチエックされるべきであるかということを決定する。例えば、Ｋ２＝１である場合には、デイジット１乃至６がチエックされ、Ｋ２＝４であるならば、デイジット４乃至６がチエックされ、そして　２＝６であるならば、最低位桁デイジットのみがチエックされ、従つてチエックされるデイジット数が多くなる（即ち、Ｋ２が小さくなる）につれて、主データ処理システムとオフ・ラインで動作している場合には、ＩＤ番号を推量することから生ずる保護の誤りが増大する。しかしながら、端末装置内でのみチエックされる諸デイジットはクレジット・カードの情報と予め決められた対応を有していなければならないが、チエックされないデイジットはこのような対応を持たなくてもよい。従つて、端末装置でのみチエックされるクレジット数が増えれば、チエックされないデイジット数は減少され、対応付けアルゴリズムと暗号化用キーとの間で妥協がなされる場合には主データ処理システムとのオン・ラインの動作時にデータ・ベースへアクセスする機会は増大される。この例に対しては、Ｋ２＝４で端末装置のみでのチエック用特徴部分を選ぶことによつて顧客は自分の随意選択事項を選んでいる場合が想定される。

ＩＤ番号とクレジット・カード情報との対応を決定する特定の暗号化アルゴリズムは、暗号化されていないテキスト入力と暗号化されたテキスト出力との関係が本明細書では第１の暗号化用キー（キーＡ）と呼ばれる暗号化用キーによつて決められねばならないということを除いて本発明を実施する上では重要ではない。この例のために、暗号化アルゴリズムは Scientific American（１９７３年５月）の第１５頁乃至第２３頁に掲載されている論文 "Cryptography and Computer Privacy"、又は Computer Design（１９７４年４月）の第１２９乃至第１３４頁に掲載されている論文 "Enciphering Data for Secure Transmission" に記述されている型式のアルゴリズムであるとする。アルゴリズム１０６のための暗号化用キー例えばキーＡは６４の２進デイジットを含むワードである。この暗号化用キーは又８つの８ビット・バイトを含むものとして考えられてもよい。キーＡはオペレータ用機能サブシステム７６の補助メモリ部分に貯えられ、その中の１２８メモリ・ワードの中の８メモリ・ワードを占める。このキーを完全に保護する為に、顧客インターフエイス・パネルから保守作業が要求される度毎に上記キーは破壊される。１つの構成においては、保守員が端末装置の保守作業を完了するまでキーＡにアクセスしうることを許された銀行員は待機しており、然る後にシーケンシヤル

に入れられる8つの16進デイジット対として64ビット・コードを上記メモリへ入れる。最新に送り込まれた2デイジットを任意の与えられた時刻に表示してもし必要ならば送り込まれたデイジットを正すように、オペレータ用パネルの16進表示装置はその送り込まれたデイジットを表示する。2デイジットだけに表示を制限するのは、そのキーの安全性を確保することにあり、これはキーの表示を見てそのキーのコピーをとろうとする人に対してそのキーの送り込みが完了されるまでに一瞬時たりともキー全体を見させなくすることによつて担保される。キーが一旦送り込まれると、そのキーは再度表わされることはない。このようにして、キーAを直接に端末装置に入れることが可能になるのである。

しかしながら、他の例においては、信用のある銀行員はキーAではなくて、キーAに予め決められた関係を有するキーA'を与えられる。この場合にも、その信用のある銀行員はキーAを入れると全く同じ方式でキーA'を端末装置へ入れる。しかしながら、端末装置は暗号化アルゴリズム106に類似していてもよいし、全く同じであつてもよい暗号化アルゴリズム108でキーA'を処理して暗号化用キーAを作り出す。暗号化アルゴリズム108は暗号化プロセスにおける端末装置用支援キーであり、キーA'をキーAへ変える第2の暗号化用キー(キーCと呼ぶ。)を用いる。代替として、完全に別個のキーがこの目的のために初期設定時に送り込まれてもよい。

キーAで暗号化されるクレジット・カードのデータの内の32ビットと、そのクレジット・カードが手渡される時にその顧客へ割り当てられた6デイジットの顧客ID番号との予め決められた関係のためにキーAの安全性を確保することは極めて重要である。或るクラスのクレジット・カードはそのクレジット・カードで取引している銀行の1より多くの支店で用いうるようにするためには、必要なときに端末装置46でキーAにアクセスされうるように、各々の支店で少なくとも1人の人がキーAにアクセスし得なければならない。多数の支店を有する大きな銀行におけるこの分配は非常に広範囲になる。更に、クレジット・カードが1より多くの銀行の間で交換可能に利用しうるようにするためには、そのクレジット・カードを受取るすべての銀行は同一の暗号化用キーAを有していなければならない。キーAにアクセスしうる人数が更に増大され、そのために安全性の確保に関する問題が生ずる。暗号化アルゴリズムを使用すれば、キーAの広範囲な分配に対しキーAのための安全性が確保される。銀行毎に異なるキーCを使用すれば、与えられたキーCに対応する予め決められたキーA'が首尾よく処理されて非常に重要なキーAを作りうる。例えば、各々の銀行は3つ若しくは4つの端末装置14を有する別個の支店を有するものとする。その銀行又はその支店のためのキーA'のみが首尾よくキーAを作り出す。1つの支店でキーA'へアクセスしうる人が、暗号化アルゴリズム108で異なるキーCが用いられている異なる支店へ行つたとしても、第1の支店でのキーA'は第2の支店ではキーAを作り出し得ない。従つて、キーAを限られた非常数少ない高度に選ばれた人達にだけ与えるようにすることが可能である。

かくして、暗号化アルゴリズム106は出力として32ビット入力に対して予め決められた関係を有する32ビットを発生する。これらの32の出力ビットは30ビットのみが用いられる状態でテーブル変換プロセス110で6つの5ビット・ワードに分けられる。例えば、各々のワードは最後の方の2ビットを使用せずに各々シーケンシャルな5ビットから成る初めの方の6グループから形成されるのがよい。各々5ビットから成る各グループは各々のアドレス・ロケーションに値1乃至9の内の1つの10進デイジットを貯えるテーブルをアクセスする際のアドレス・ワードとしてテーブル変換処理110で用いられる。このようなテーブル変換は各々値1乃至9を有する6デイジットを発生する。これらのデイジットは顧客ID番号に対し直接的な対応を有しており、デイジット0は、先導する一連の0で始まり、混乱し又は

可変長の処理内容を生じさせると予想されうる顧客ＩＤ番号を避けるために、除かれる。

クレジット・カード上の情報が妥当であるということが見出されるならば、顧客用アクセス・パネルが開かれ、顧客用の光学的表示装置及びキーボード１１２への顧客によるアクセスが可能になる。顧客は該キーボードの数字フイールドから自分のＩＤ番号を打込む。顧客が予め決められた時間内に６デイジットを正しく打込まないならば、既に打込んでいるデイジットは正しくないＩＤ番号とみなされ、再打込みが指示される。６デイジットが正しく打込まれると、打込まれたＩＤ番号の一部若しくは全部が随意にテーブル変換処理１１０によつて発生された６デイジットの番号と比較される。対応する６デイジット対の内のどのデイジット対が比較されるべきであるかということを、キーＫ２が指定する。

この例において、Ｋ２＝４であるものとするならば、位置４、５及び６を有する３つのデイジットが比較ステップ１１４で比較される。比較が首尾よい比較結果を示さないならば、打込まれたＩＤ番号が誤つているということが表示され、その顧客は自分のＩＤ番号と再打込みするように指示される。ＩＤ番号が所定回数例えば３回の中に正しく打込まれないならば、取引要求が終了され、メッセージが主データ処理システムへ送られる。主データ処理システムからコマンドに応答して、盗難にあつたと思われるクレジット・カードのＩＤ番号と一致するように上記顧客のクレジット・カードを更に何回も繰返して使用するのを防ぐために上記顧客のクレジット・カードは好ましくは保管所へ送られるのがよい。又は、そのクレジット・カードは顧客へ返却されるのがよい。キーボードから打込まれたＩＤ番号の諸デイジットがこれに対応するクレジット・カードから得られたデイジットと一致するということが判ると、顧客ＩＤ番号の６デイジットがステップ１１６で３２ビットの２進コードへ変換される。ステップ１１６においては、上記２進コードの初めの方の２４ビットは打込まれた６デイジットから直接に得られる。

シーケンシヤルな各々の４ビット・デイジット対を単一バイトとして取扱いそして既に現われている３バイトの各々に関して対応するビット位置の相継ぐ排他的オアを取つて第４番目のバイトの対応するビット位置のデータ内容とすることによつて、最後の８ビット即ち１バイトが得られる。打込まれたＩＤ番号のすべてのビットの関数である可変情報を発生する限り、最後の８ビットに関する情報を得る他の手段が用いられうる。これらの３２ビットはキーＡを使う暗号化アルゴリズム１１８で処理されて暗号化された３２ビットの顧客ＩＤ番号を作り出す。暗号化アルゴリズムは一般に任意の適当な暗号化アルゴリズムであつてもよいが、この例においては暗号化アルゴリズム１１８は暗号化アルゴリズム１０６と同じものとする。両暗号化プロセスに対し同一のアルゴリズムを使用すれば、両プロセスに対して同一の貯えられたプログラム若しくはハードウエアの論理回路を用いうることが出来る。アルゴリズム１１８のための暗号化用キーは又一般には任意の適当なキーであつてもよい。しかしながら、この例に対しては、アルゴリズム１１８はアルゴリズム１０６で用いられるキーＡと同じキーＡを用いるものとする。同一の暗号化用キー及び同一の暗号化アルゴリズムを重複して用いれば、端末装置１４の動作の複雑性は緩和され、必要とされるデータ貯蔵装置の容量は減少される。このようにして暗号化アルゴリズム１１８から発生される３２ビットは一度暗号化された顧客ＩＤ番号を表わしている。

暗号化された顧客ＩＤ番号を表わす３２ビットはステップ１２０において、２つの４ビット・デイジットを用いないようにして、６つの４ビット・デイジットへ変換される。ステップ１２２において、無視された２つのデイジットは可変データの２つの４ビット・デイジットと置き換えられる。ＩＤ番号から導かれた情報と可変情報とのこの置き換えは暗号化されたフイールドを不変量にさせない。一般に、可変データは顧客ＩＤ番号に予め決められた関係を有せず、且つ各々の取引要求メッセージで変わる任意のデータであつてよい。こ

の良好な実施例においては、可変データは現金支払取引のための現金カウンタ（ＣＮＴＲ）及び他の取引のための取引番号（Ｎ）である。

６つの４ビット・デイジットと８ビットの可変データとの組合わせから成る３２ビットは第３の暗号化用キーＢを用いる暗号化用アルゴリズム１２４を通過される。暗号化用アルゴリズム１２４は一般に任意の適当な暗号化用アルゴリズムであつてよい。しかし、この良好な実施例に対しては、アルゴリズム１２４はアルゴリズム１１８、アルゴリズム１０６、及びアルゴリズム１０８と同じであるものとする。キーＢは６４ビットの暗号化用キーであり、該キーは初期設定中に主データ処理システム１２から受け取られ、新しいキーが主データ処理システムから送られて来ない限り変えられることはない。暗号化アルゴリズム１２４は３２ビットの暗号化されたデータを生じさせ、この暗号化されたデータは上述の４バイト・ヘッダ・フィールドに直続して取引要求メッセージの中に組立てられる。

比較ステップ１１４がクレジット・カードを少なくとも部分的にその妥当性を見出した後、顧客はキーボード１１２を使うことによつて要求している取引を進めるように指示される。先ず、顧客は要求しつつある取引の形式を指示するように命令される。キーボードの取引要求フィールド内のすべてのバック・ライトは点灯されている。特定のキー例えばfunds transferキーが押圧されると、該キーのバック・ライトのみが点灯されたままにあり、その他のすべてのキーのバック・ライトは消灯される。然る後に、顧客は資金を１つの勘定から他の勘定へ移したい該１つの勘定を選択するように合図される。この時刻には、預金勘定フィールド内のすべてのキーのバック・ライトが点灯されている。顧客が貯金勘定キーを選ぶと、該キーのバック・ライトだけが点灯されたままにあり、預金勘定フィールド内の他のすべてのキーのバック・ライトは消灯される。然る後に、顧客は資金を移したい上記他の勘定を選択するように合図される。この時刻に、その移し先の勘定フィールドのすべてのバック・ライトが点灯されている。checking accountキーを選ぶならば、該キーのバック・ライトが点灯されたままにあり、移し先の勘定フィールドの他のすべてのキーのバック・ライトは消灯される。点灯されているバック・ライトは顧客が自分の取引要求のためキーボードから入れたステータスを確かめる若しくは思い出させるための確認表示を与える。顧客は新しいキーを押圧したい既に押圧済みのフィールドへ戻り、該フィールドからキーボードからの打込み過程を続けることによつて自分の取引を変更しうる。数値情報例えば移したい資金のドル高はキーボード１１２の数字フィールドから打込まれる。顧客ＩＤ番号を除いて打込まれるすべての数値情報は確認のため表示される。顧客の後に立つている人に該顧客のＩＤ番号を不正に知らしめないために顧客ＩＤ番号は表示されない。キーボード・データ、磁気記録帯から読取られるクレジット・カード・データ、並びに任意所望の付加的なデータは４バイト共通ヘッダ・フィールド及び４バイトの暗号化されたフィールドに続いてクリア・テキストの形で続けられる。然る後に、この情報は伝送部１２６において取引要求メッセージとして主データ処理システムへ送られる。

2.取引応答メッセージ

第４図を参照すると、取引要求メッセージが主データ処理システムによつて受取られるにつれて、該メッセージは分離処理部１４０へ与えられる。該処理部１４０は種々のデータ・フィールドを分離するように動作し、共通ヘッダ・フィールドはメッセージ・ルーティングのために使用され、暗号化された３２ビットは暗号解読化アルゴリズム１４２を通され、クリア・テキストは大容量データ貯蔵装置１４６を有する主データ・プロセッサ１４４によつて受取られる。暗号解読化アルゴリズム１４２はキーＢを使用するが、該キーは暗号化アルゴリズム１２４で用いられた第３の即ち伝送用キーと同じである。主データ・プロセッサ１４４はデータ貯蔵装置１４６をアクセスするのにクリア・テキストのデータを用いる。データ貯

蔵装置１４６は勘定データ並びに顧客のクレジット・カードに関連付けられる情報例えば暗号化された顧客ＩＤ番号（若しくは諸番号）を含む。

暗号解読化アルゴリズム１４２によつて発生される３２ビットは分離プロセッサ１４８を通過され、そこにおいて暗号化された顧客ＩＤ番号の６つの４ビット・デイジットは２つの可変デイジットから分離される。分離プロセッサ１４８からの６デイジットと暗号化された形式で貯えられているデータ貯蔵装置１４６からのＩＤ情報の６デイジットとの比較を比較部１５０で遂行する。

この暗号化プロセスはオン・ラインの主データ処理システムと通信している種々の端末装置１４に貯えられている現金の安全性を非常に改善する。クレジット・カードの勘定番号と顧客ＩＤ番号との対応を所在しうる悪意の人は端末装置１４から現金を不正に得ることが出来よう。例えば、或る人が実際の顧客勘定に属するところの情報を記録しているクレジット・カードを偽造するか又は盗むことがある。偽造したクレジット・カード及び対応する顧客ＩＤ番号を使えば、或る人がクレジット・カードを介してアクセスしうる種々の貯金勘定、小切手勘定若しくは他の勘定の残高に関して先ず問い合わせうる。その残高情報が得られたならば、その人はクレジット・カード及び現金支払端末装置１４を用いて、上記夫々の勘定に関する金額又は端末装置の現金がなくなるまで現金をこれらの勘定から引出しうる。現金支払端末装置にあるすべての現金が支払われてしまうまでそれらのクレジット・カードの有する他の勘定及び対応する顧客ＩＤ番号が類似の方式で利用されうる。このような場合には、付加的な諸クレジット・カード及び顧客ＩＤ番号を使つてそのシステム内の他の現金支払端末装置から現金を全部引出すために、その人は上記他の現金支払端末装置へ出向くことになる。各々の現金支払端末装置１４は何千ドルもの現金を保有し得、又主データ処理システム１２と通信する多数の端末装置１４がありうるから、クレジット・カードの勘定番号と安全性を確保された顧客ＩＤ番号との対応を維持し、然かも端末装置内でのチエックを施行してオフ・ラインでの使用を通して端末装置１４のより高度の利用性を可能にすることが極めて重要になる。本明細書で説明した諸技法を用いれば多数の勘定のための、クレジット・カード情報と顧客ＩＤ番号との対応を、或る人が得ることは極めて難しくなる。たとえ顧客ＩＤ番号が貯えられたクレジット・カード情報を暗号化アルゴリズム１０６を通すことによつて完全に発生され得たとしても、その暗号化用キーＡの安全性は上述したように維持される。

顧客ＩＤ番号の一部（又は、好ましくは全部）例えば初めの方の３デイジットと貯えられたクレジット・カード情報との関係が予め決められた関係にないならば、そのシステムの安全性をくずすことが更に一層難しくなる。主データ処理システム１２のためのデータ処理センターにいる人が貯えられている暗号化されたＩＤ番号をアクセスしたいことが起こりうる。しかしながら、実際の顧客ＩＤ番号は主データ処理システムには貯えられておらず、そして端末装置１４のキーボードから打込まれねばならないのは実際の顧客ＩＤ番号であるから、端末装置１４から現金を得るのには暗号化されたＩＤ番号は価値がない。従つて、主データ処理システムのデータ・ベースに貯えられている暗号化された夫々の顧客ＩＤ番号と暗号化アルゴリズム１１８に対応する暗号解読化アルゴリズム及び暗号化用キーＡとの双方へアクセスするためには、多数のクレジット・カードの情報と対応する顧客ＩＤ番号との対応を、その対応を求めている人が得ることが必要になる。

クレジット・カードが顧客へ手渡されるとき、クレジット・カード情報と顧客ＩＤ番号との対応を知つている人を非常に少ない人に限ることが可能である。実際には、顧客ＩＤ番号の一部をクレジット・カード情報から導き、他の一部をコンピュータにより発生するようにして取引勘定は確立される。完全な顧客ＩＤ番号は然る後に印字されそしてクレジット・カードと共にその顧客ＩＤ番号を印字した用紙を封筒の中に入れ密封してその顧客に手渡される。そうすれば、端末装置１４によつて処理されるクレジット・カード勘定につき

取引したいときにその顧客が上記封筒を開封すれば上記の完全な顧客ＩＤ番号をその顧客は目で見ることが出来る。このようにして、銀行と取引きのあるどのような人もクレジット・カード勘定とこれに関連付けられる顧客ＩＤ番号との対応をアクセスし得ない如き安全性の高いシステムを作ることが可能である。

貯えられている暗号化された顧客ＩＤ番号と暗号化されて送られて来た顧客ＩＤ番号とが同じでないということを比較部１５０が示すならば、主データ処理システムはその取引の実行が認容されないということを示す取引応答メッセージを組立て、そして端末装置へ送る。該取引応答メッセージは顧客のクレジット・カードを保管するかその顧客へ返すように取引の要求を出している端末装置を指揮する。逆に、上記の２つの暗号化されたＩＤ番号の間の対応が見出され、そして要求した取引が保有している金額、引出し高、又は勘定残高に関係する任意に予め決められた規則に違反しないならば、その取引は取引応答メッセージによつて認容される。取引応答メッセージは端末装置から送られて来た取引要求メッセージの中の３２ビットからなる暗号化された情報に対応する３２ビットから成る暗号化された情報を含む。組立て処理部１５２において、３２ビットが組立てられ、キーＢ（第３の即ち伝送用の暗号化用キー）を用いる暗号化アルゴリズム１５４で暗号化される。この暗号化アルゴリズムは一般には、任意の適当な暗号化アルゴリズムであつてもよいが、この例に対しては、暗号化アルゴリズム１５４は暗号化アルゴリズム１０６、１１８及び１２４と同じであるものとする。更に、キーＢは暗号化アルゴリズム１２４のためのキーＢと同じであるものとする。暗号化して組立てられた３２ビットは６デイジットの暗号化されたＩＤ番号及び２つの可変デイジットを含む送られて来た３２ビットとは異なる。取引応答メッセージの中のこの３２ビットは端末装置１４で取扱われ発行される請求書毎に増分される第１の現金カウント（ＣＮＴＲ１）に対応する１バイトの現金カウンタ数値、端末装置１４が顧客の要求した取引に対し取るべき応答を示すアクション・バイト、現金カウントを同定し端末装置１４内の第２の現金支払機構のために維持される第２の現金カウンタ・バイト（ＣＮＴＲ２）、並びに要求した取引に関係する請求書数を示す数量バイト（ＡＭＴ）を含む。然る後に、これらの３２ビットは暗号化アルゴリズム１５４で処理されて暗号化された３２ビット１５６を形成する。それから、この暗号化された３２ビット１５６は取引を完成させるのに必要なクリア・テキスト・データ例えば随意表示データ、随意受領データ、若しくは付加的なデータと結合され、そして伝送部１５８において取引応答メッセージとして要求を出している端末装置４６へ送られる。

３取引の実行及びステータス・メッセージ

取引応答メッセージが端末装置１４で受取られるとき、該メッセージは伝送の正しさをチエックし、メッセージを種々のフイールドへ分ける入力処理部１６０へ入る。その暗号化されたフイールドは暗号解読化アルゴリズム１６２へ送られる。該アルゴリズムはキーＢを使つて、１バイトの現金カウンタ１（ＣＮＴＲ１）、アクション・バイト、１バイトの現金カウンタ２（ＣＮＴＲ２）及び１バイトの数量データ（ＡＭＴ）を含む３２ビットに直す。これらのバイトは、取引応答メッセージがエラーなしに受取られ、端末装置から送られた正しい取引要求メッセージに対応していることを保証するように、それらの正しさについてチエックされる。取引終結部１６４が取引応答メッセージの話内容に従つてその取引を実行する。取引の実行において、端末装置１４はクレジット・カードを返すか又は保持し、適当な取引書例えば現金取引書若しくは他の印字した取引書を発行し、その取引を正式に実行するか又は取消し、顧客による受認又は非認を与えるように適当なメッセージを表示し、そしてその取引の完了に必要な他の任意の諸取引実行機能を遂行する。

顧客が要求した取引の完了時に、端末装置１４は要求した取引の終了の仕方、及び端末装置１４のステータスを主データ処理システム１２へ知ら

せるステータス・メッセージを主データ処理システム１２へ送る。ステータス・メッセージを用意するための３２ビット組立部１６６があり、該組立部からの３２ビットはキーＢを使う暗号化アルゴリズム１６８で暗号化されて暗号化された３２ビット１７０を発生する。暗号化アルゴリズム１６８は一般には、任意の適当な暗号化アルゴリズムであつてもよいが、良好な実施例に対しては、暗号化アルゴリズム１０６、１０８、１１８、１２４、及び１５４と同じである。キーＢは暗号化アルゴリズム１２４及び１５２のためのキーＢと同じである。しかしながら、キーＢはキーＡと異なつて主データ処理システムによつて変えられうるのがよく、従つてキーＢは時間の経過と共に必要とするキーに変えられるということが認められよう。３２ビット１７０は出力処理部１７２へ送られ、そこにおいて暗号化されないステータス情報と結合させ、そしてステータス・メッセージとして、取引を実行した端末装置から主データ処理システム１２へ伝送される。

本明細書で説明したように、暗号化アルゴリズムを使用する方法は複数の暗号化プログラムを貯えるための貯蔵容量を必要とすることなしに取引実行システム１０のための安全性を高く保て得る。更に、暗号化アルゴリズムと暗号解読化アルゴリズムとを適正に選べば、暗号解読化アルゴリズムは暗号化アルゴリズムと殆んど同じであつてよく、従つて暗号化及び暗号解読化の双方に対し暗号化アルゴリズム・プログラムの大部分を使用しうる。このことはプログラム貯蔵容量を更に節約しうる。顧客の取引のための３つのメッセージに対し同一フォーマットを利用しているが、これらのメッセージの中の３２ビットから成る暗号化された情報に対する最後の暗号化処理は通信路を経て伝送される暗号化されたＩＤ番号の安全性を確保することにある。取引要求メッセージにおいて、組立処理部１２２が暗号化されたＩＤ番号と可変データとを結合するが、これは通信線をモニタする人が同一のＩＤ番号及びクレジット・カード情報、繰返して入れ、そして取引要求メッセージを繰返して送り、そして対応する暗号化された通信内容をモニタすることによつて、キーＢ及び暗号化アルゴリズム１２４を見破るのを極めて困難にすることにある。取引応答メッセージはカウンタ１のバイト、アクション・バイト、カウンタ２のバイト、及び数量バイトを含む。この情報は取引要求メッセージのエンコードされた情報とは全く異なり、又可変情報を含む。数量バイト及びアクション・バイトは取引要求メッセージと同一形式のため同じになる傾向を有するが、制御バイトは変わる。ステータス・メッセージの暗号化された３２ビットは、他の２つのメッセージの中のいずれの暗号化されたフイールドとも異なるが、これはこれらの２つのメッセージが時間と共に変わる取引番号、並びに取引応答メッセージに対しては異なるバイト位置に置かれるカウンタ２のバイト及びカウンタ１のバイトを含み、通常のステータス・メッセージに対しては（２進カウントで）ステータスの番号を示すカウント・バイト（ＣＢ）及びメッセージの暗号化された部分に続く複数の問合わせデータ・バイトを含むからである。取引の終了に応答して発生されるステータス・メッセージは通常、問合わせデータ・バイトを含まない。ステータス・メッセージが回復要求型の例外ステータス・メッセージである場合においては、暗号化されたフイールドの第３バイト（ＣＢ）は最後の取引要求メッセージに対する取引応答メッセージからのアクション・バイトを含む。従つて、キーＢを時間の経過と共に必要に応じて変え、異なる形式のメッセージの各々の暗号化部分の中に異なる情報を入れて伝送するならば、通信線をモニタすることによつて伝送用暗号化アルゴリズムを見破りその時点で用いられているキーＢを見出す作業は極めて困難にされる。たとえ伝送用暗号化アルゴリズム及びキーＢが見破られたとしても、諸メッセージの伝送をモニタすることによつては、その伝送がモニタされつつあるときに使われている特定のクレジット・カードに対するそのクレジット・カード勘定と暗号化された顧客ＩＤ番号との間の対応のみが知り得るだけである。多数の偽造

若しくは盗難のクレジット・カード情報と対応するＩＤ番号との対応は更にキーＡを見出すことによつてのみ達成される。顧客ＩＤ番号のすべてのデイジットとクレジット・カード上の情報との間の予め決められた関係がある代替の実施例においては、データ・ベースへのアクセスは必要でない。端末装置内における随意的なＩＤ番号のチエックが施行される場合には、勿論、キー Ｋ1及びＫ2は暗号化されたＩＤ番号に対する安全性を更に高める。

4. 図面の簡単な説明

第１図は本発明に従う取引実行システムのブロック・ダイヤグラム。第２図は第１図に示される取引実行システムに使用される取引用端末装置のブロック・ダイヤグラム、第３図は顧客の開始した取引要求が取引用端末装置によつて初期的に処理される様式を表わすブロック・ダイヤグラム、第４図は取引用端末装置から送られて来る取引要求メッセージが主データ処理システムによつて処理される様式を示すブロック・ダイヤグラム、第５図は主データ処理システムからの取引応答メッセージが取引用端末装置によつて処理される様式を表わすブロック・ダイヤグラムである。

１００……クレジット・カード、１０２……クレジット・カード読取機構、１０６……暗号化アルゴリズム、１１０……テーブル変換処理、１１２……キーボード、１１４……比較手段、１１８及び１２４……暗号化アルゴリズム、１２６……伝送部、１４０……分離処理部、１４２……暗号解読化アルゴリズム、１４４……主データ・プロセッサ、１４６……大容量データ貯蔵装置、１４８……分離プロセッサ、１５２……組立処理部、１５４……暗号化アルゴリズム、１５８……伝送部。

出願人　インターナショナル・ビジネス・マシーンズ・コーポレーション

代理人　弁理士　小　野　廣　司

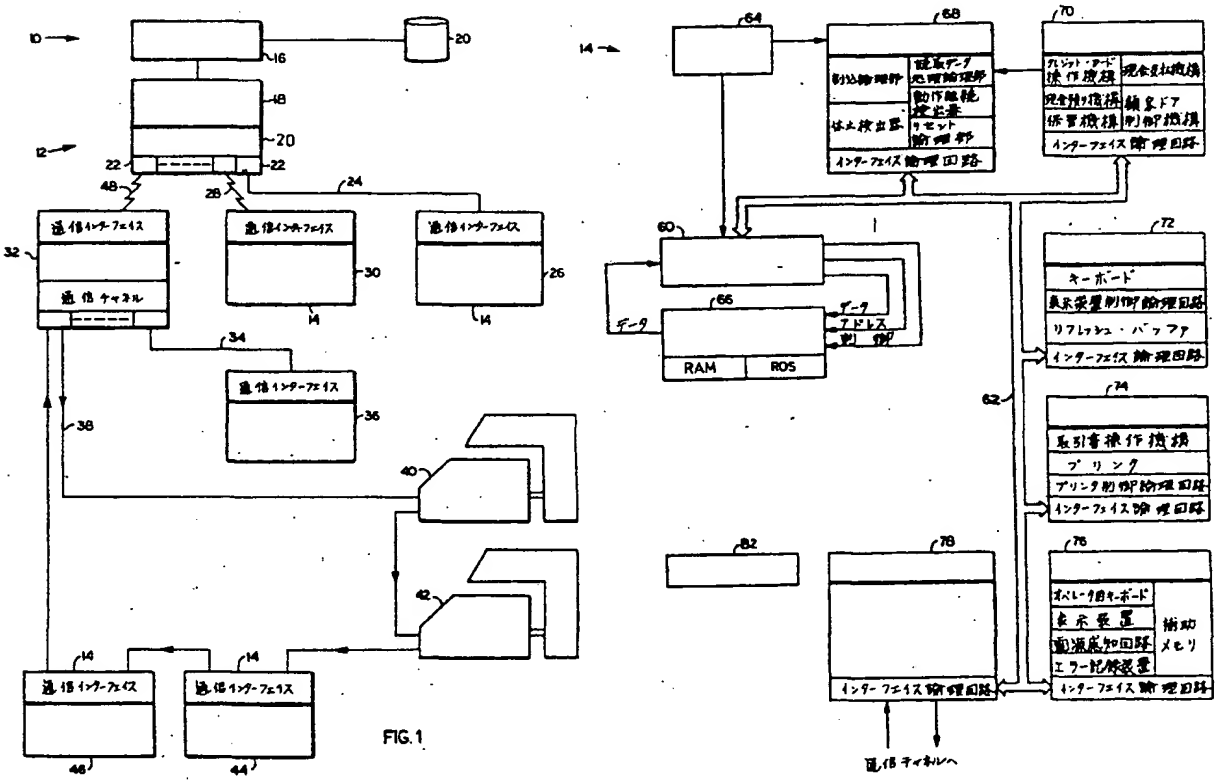

FIG. 1

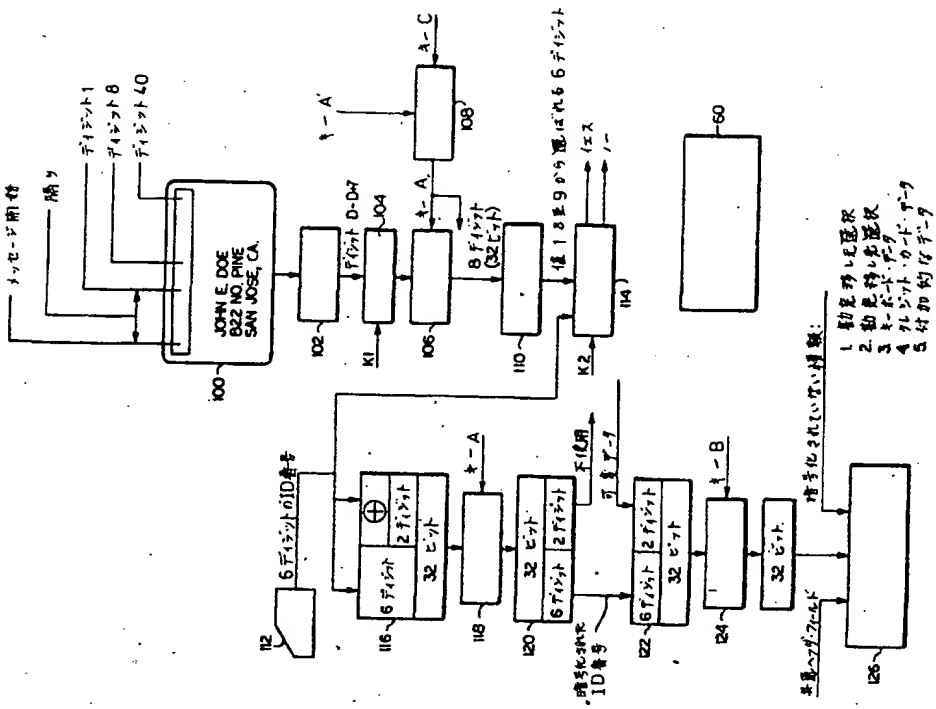
JOHN E. DOE
822 NO. PINE
SAN JOSE, CA.
100
102
104
106
108
110
112
114
116
118
120
122
124
126
60
K1
K2
A
B
C
D-D7
32 ビット
6 ディジット
2 ディジット
8 ディジット (32 ビット)

FIG. 3

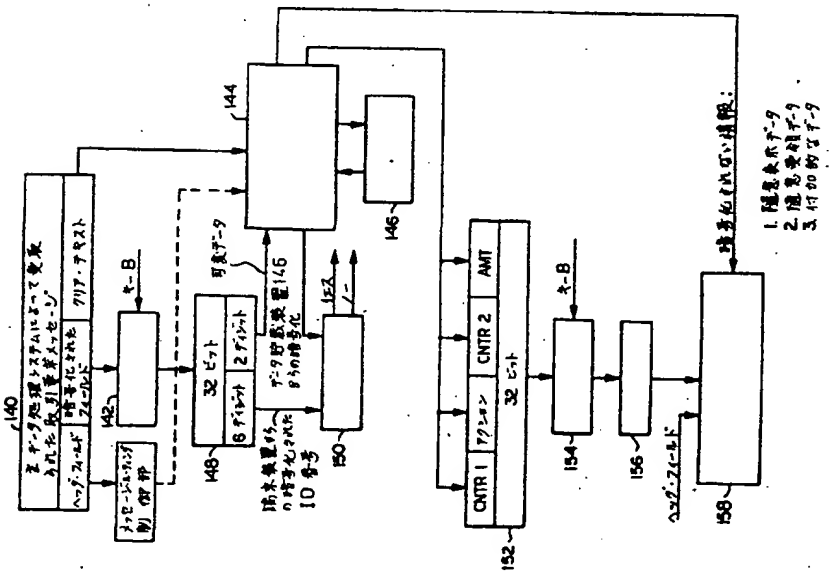
140
142
144
146
148
150
152
154
156
158
CNTR 1
CNTR 2
AMT
32 ビット
6 ディジット
2 ディジット

FIG. 4

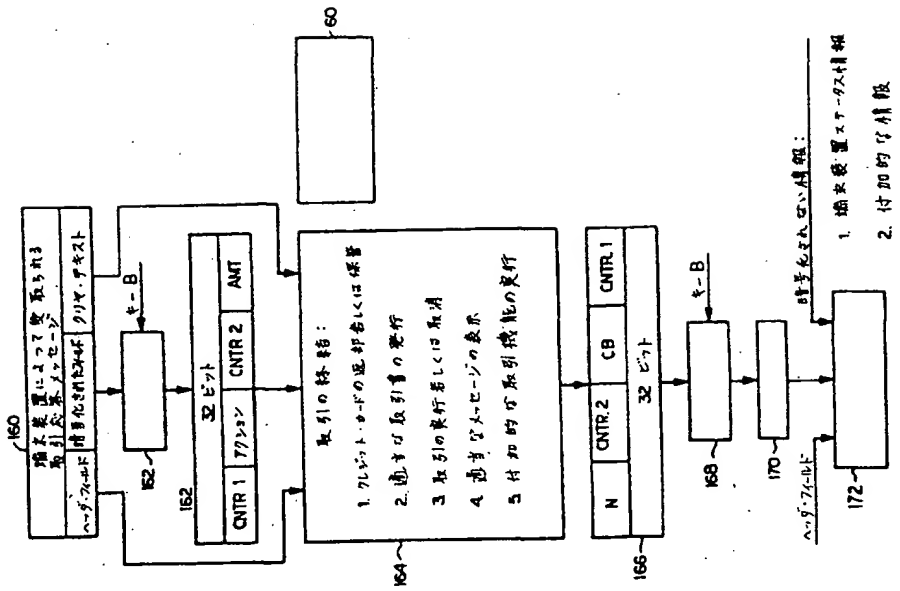

FIG. 5

6 前記以外の発明者又は代理人

(1)発 明 者

住 所 アメリカ合衆国カリフォルニア州サン・ホセ、ラデイアント・ドライブ6240番地

氏 名 ウイリアム・エイ・ブースロイド

住 所 アメリカ合衆国 カリフォルニア州サン・ホセ、アンナ・ドライブ 4930 番地

氏 名 リチャード・シー・フレイ